Dissertation

Personal Information Protection and Rational Utilization in Space-time-behavior Analysis Based on Big Data

Graduate School of

Natural Science & Technology

Kanazawa University

Division of Environmental Design

Student ID No: 1824052011

Name: LIN YONG

Chief Supervisor: Professor SHEN ZHENJIANG

September, 2021

Abstract

With the rapid development of Internet of Things, 5G mobile networks, Cloud Computing, Artificial Intelligence and other information technologies, human society has entered the era of big data. With the continuous advancement of information construction, it not only promotes social development and technological change, but also brings new challenges to the protection of personal information. When the big data is mined and utilized by all kinds of stakeholders, the abuse of personal information brings lots of privacy leakage and economic loss. This dissertation focuses on the protection and rational utilization of personal information in space-time-behavior analysis in the era of big data. First of all, the concepts about the protection on personal information in the big data era are discussed. Identifiability, idiosyncrasy, relativity are three important characteristics of personal information. Subsequently, the specific legislative forms and supervision modes of personal information protection in major countries are compared, and the common trend of legislation is to seek a balance between personal information protection and rational utilization. Informed consent is the basic principle of personal information protection all over the world. However, in the era of big data, information overload, status asymmetry, data explosion and rapid transmission are challenges to the principle of informed consent. Anonymization, rational expectation and public interest use are the rules of personal information protection and utilization, and are the supplements of the principle of informed consent. This work has published in *Proceedings of International Conference 2019 on Spatial Planning and Sustainable Development*, Aug. 30th-Sept. 1st, 2019, Chiba University, Japan.

Mobile phone signaling big data is widely used in spatio-temporal planning and management. The mobile phone signaling big data not only has space and time dimensions, but also has significant human behavior attributes. It is used for building the dynamic analytical framework of urban planning based on "space-time-behavior". Even though the mobile phone signaling big data has been anonymized, it still unavoidablely displayes a lot of special position attribute information of mobile subscribers. The anonymous trajectory data would be matched to the relevant geographic spatial, thereupon then to reveal the information subject's active position information in a special time. Therefore, it can conveniently identify the special position information, for example, the work and living place of users, and go so far as to give their portraits. Now available technologies indicate that mobile phone signaling big data can be de-anonymized easily, so anonymization rule is inapplicable to the sharing of mobile phone signaling big data in the spatio-temporal planning. Mobile phone signaling big data can generate people's activity trajectory, which belongs to sensitive personal information. Once being divulged or misused, it may be prone to violate personal privacy and cause personal and property losses. For this reason, if just use the existing anonymous method to share the mobile phone signaling big data, it is not sufficient to defend the safety of personal information in the urban planning. Sharing the mobile phone signaling big data should adhere to the basic

principle of informed consent other effective rules of personal information protection. This work has been published in *International Review for Spatial Planning and Sustainable Developmen*t, 2021,Vol. 9(2):76-93. (ESCI, SCOPUS)

Personal information has many values involving with personality dignity and freedom, economic use, and public management. Among them, personality dignity and freedom is the core value. In the era of big data, personal information has been widely shared and used, which facilitates personal life, social production and public management but also brings the risk of personal information abuse. Meanwhile, the stakeholders relevant to personal information have become more and more diverse, leading to increasingly urgent demand for sharing and using personal information. With the great improvements in the processing efficiency and transmission rate of personal information, it has become much easier to share personal information, which makes the application of the principle of informed consent more difficult. In this circumstance, "rational expectation" becomes a new option of personal information protection and rational utilization. Through the analysis of the value of personal information and the measurement of interests, it assesses the risk of personal information sharing and utilization based on special application contexts, and discusses the criteria of rational expectation, to strike a balance among personal information protection, digital economic development and public interest maintenance, so as to drive digital innovation, economic development and social progress, as well as to effectively protect personal information. This work has been accepted by *International Review for Spatial Planning and Sustainable Development*, Expected January 2022, 20 pages. (ESCI, SCOPUS)

In smart campus, during the period of COVID-19 pandemic, universities may use personal information rationally to balance the needs of teaching devices and services, guide students' good learning behavior and healthy life behavior, ensure education and management quality. Usually, universities will postpone the opening date of campus and conduct online education when the pandemic is severe, will increase efficiency in campus management and start offline education when the pandemic is slow down. In current online education, the rational use of personal information will effectively improve the teaching quality. In current offline education, measures taken to prevent and control the pandemic need a lot of personal information, such as travel schedule, travel purpose, health information and so on. Based on crucial public interests, such as COVID-19 pandemic prevention, universities can make rational use of students' personal information. But because it involves personal privacy, it is necessary to strengthen the personal information protection both online and offline education. The more effective application of personal information, and the combination of online and offline education (e.g. LMS teaching), will help to balance the use of public teaching devices and services and improve the quality of education. This work has been published in *Proceedings of International Virtual Conference 2020 on Spatial Planning and Sustainable Development*, February 6-7th, 2021, https://www.spsdcommunity.org/spsd2020-vc/.

Key words: personal information, Protection and Rational Utilization, space-time-behavior analysis, big data, informed consent, anonymization and de-anonymization, rational expectation, crucial public interest, interest balance

Acknowledgement

The study and life in Kanazawa University is intense and full, which is unforgettable forever. Kanazawa is a famous city with a long history and rich culture. In Kanazawa University, the beautiful campus, the excellent learning environment, the knowledgeable professors and the friendly Japanese friends all left a good impression on me. As a social doctoral student in the International Collaboration SPSD Laboratory of Fuzhou university and Kanazawa University, I not only have to complete my work, but also study in the lab. I have fully witnessed the good cooperation between the two universities and the friendship between China and Japan.

First of all, I would like to thank my supervisor, Prof. SHEN Zhenjiang. No matter in the daily research, or in the process of writing doctoral dissertation, Prof. SHEN has given careful guidance. I will never forget his diligent and outstanding academic spirit. What I learned from him is not only solid professional knowledge and rigorous research methods, but also the attitude of scholars' conscientiousness and self-discipline. All this benefits me for life. At the same time, I would like to thank Prof. IKEMOTO, Prof. NISHINO and Prof. NAKAYAMA who have taught and mentored me over the past three years. And I would also like to thank all staff who give me a lot of help in educational management affairs.

Secondly, I sincerely thank the experts of my dissertation defense committee, Prof. KAWAKAMI, Prof. IKEMOTO, Prof. ITOH and Prof. PAI, for their careful review and valuable comments on my dissertation. Without their guidance, I would not be able to successfully complete this research work.

Thirdly, I want to thank my wife, my son and my family. Because of your selfless support and dedication to our family, I would able to successfully complete my three-year doctoral study. Your encouragement is the source of my strength to keep moving forward.

Finally, I want to thank all the colleagues, classmates and friends in Japan and China, especially TENG Xiao, GUO xiao, ZHAO Lizhen, ZHANG Yuanyi, WU Xin, etc. Thank them for their continuous care, support and help.

LIN Yong

July 9, 2021

Contents

Chapter 1 Introduction

1.1 Research background

With the instant development of Information & Communication Technology (ICT), Intelligent Perception Technology (IPT), Internet of Things (IoT), artificial intelligence (AI) and other related technology, human society has started the process of "digitization". Under the situation that everything can be "digitized", large amounts of diversified and dynamic data has been produced. Big data is more and more widely used in various fields, such as social living, economic production and public management, and has become an innovative element of social development. Big data is deeply integrated with the existing industries, showing broad prospects in the fields, such as optimize the business process of enterprises, promote scientific research and higher education, ameliorate medical care and public health, improve the level of urban planning and management, provide personalized and convenient services for customers and so on.

In the late 1960s, Behavioral Geography and Time Geography began to develop, providing a unique perspective for understanding the complex relationship between human behavior and urban environment in time and space. In recent years, structural equation model, LOGIT model and spatio-temporal sequence mining methods have been introduced into the study of space-time-behavior to analyze the influence mechanism of urban space on behavior, and try to simulate and predict it. Behavior research is integrated into urban planning, and spatio-temporal big data is used to mine the spatio-temporal characteristics of human behavior, and then it is matched with geographic information space to build the basic dynamic analysis framework of "space-time-behavior". Mastering residents' space-time-behavior rules, we can make up for the shortcomings of insufficient research on urban activity system, lack of thorough analysis on residents' activity demand and little understanding of behavior decision-making mechanism, so as to make urban planning people-oriented and promote the refinement, dynamic and intelligent of urban management. Therefore, space-time-behavior analysis is a research framework to understand city based on behavior. Using information technology to analyze space-time-behavior, and realizing the construction of people-oriented city through time and space planning and behavior

guidance. Space-time-behavior analysis is not only the direct embodiment of people-oriented concept, but also the basis of big data application. By using the dynamic big data containing temporal, spatial and personal information, we can develop from the planning based on urban physical space and economic activities to the planning based on individual residents and their daily life, and from the static blueprint planning to the dynamic process planning, so as to make the urban planning and management more scientific and smart.

Smart city is an advanced concept of modern social development, is the product of the organic combination of people-oriented city and information city, which is to use big data, ICT and spatial information integration technologies to achieve the humanization, intellectualization, systematization and sustainability of urban system.[①] The core and soul of smart city planning and management is people-oriented. It is based on space-time-behavior analysis framework, makes "dynamic" analysis of urban system with the support of modern information technologies, by mining, relating, identifying, integrating all kinds of big data (especially including personal information) under the framework of laws and regulations. It combines human elements to improve the intelligence and sustainability of land space planning, natural resource utilization, urban infrastructure construction, social public service, community livelihood affairs, and so on. On the one hand, based on individual behavior, optimize the urban spatial structure (such as urban function partition) and urban time structure (such as the operation time of public service facilities) to ensure that the urban spatio-temporal structure matches the needs of residents' living activities, and provide the basic guarantee of urban material environment for the smart daily life of residents. On the other hand, facing individual behavior, it helps residents to make smart behavior decisions in daily life through soft policy and information means, and guides residents to form smart, healthy and low-carbon behavior mode and life style. Therefore, smart city planning and management includes living space planning and living time planning based on individual behavior, and behavior guidance for urban residents facing individual behaviors.(Chai, Shen, et al., 2014) The purpose of people-oriented smart city planning and management based on space-time-behavior is to realize the sustainable urban development and the smart daily life. That is to say, the humanization, intellectualization, systematization and

① *The "13th Five-Year" National Informatization Plan*, China, 2016.

sustainability of urban development, and the intelligent, healthy and low-carbon behavior mode and lifestyle of residents. (As shown in Figure 1-1)

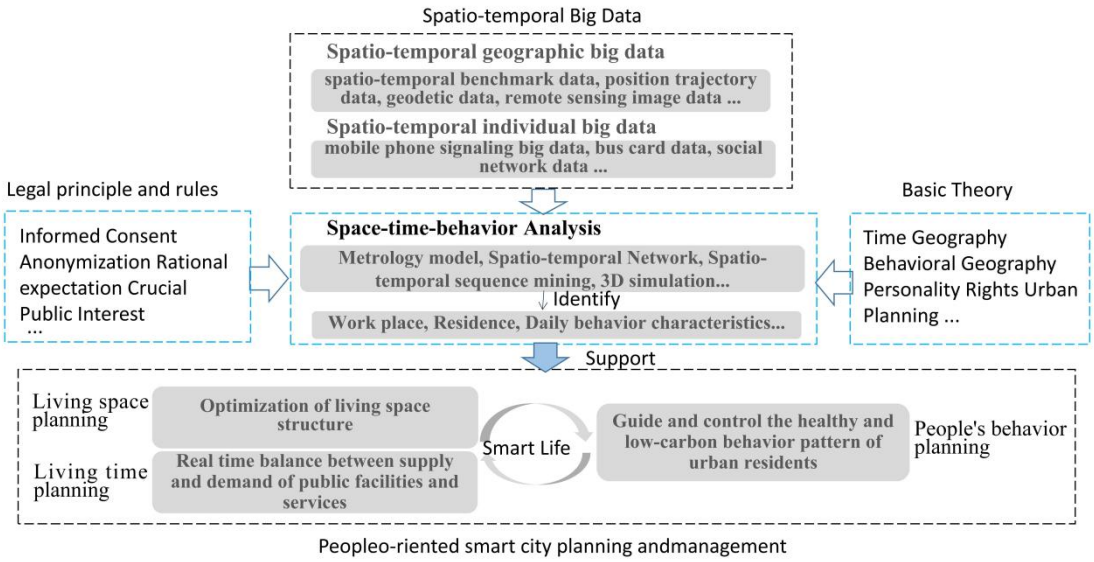


Figure 1-1 Space-time-behavior analysis framework

In space-time-behavior analysis, spatio-temporal big data is the basic supporting data. While the mobile phone signaling is the most important spatio-temporal big data. In reality, more and more organizations collect big data with actual-time location information for providing a variety of services, which brings convenience to daily life of people. In the meantime, there are also problems that personal information is illegally collected and irrational used, even leaked on a large scale, which leads to discrimination, reputation damage and personal and property injuries. In the light of the report published by the ITRC and HHS of USA, about 137 million pieces of information were leaked related to top ten information leakage incidents in 2019, and this number reached as high as 705 million in 2018. *The analysis report on the situation of information leakage of government and enterprise institutions in 2017* shows that financial websites, government websites and communication operators websites were the most vulnerable to divulgable information, accounting for 28.3%, 26.7% and 24.7% respectively. The number of vulnerability reports of websites in three major industries accounted for 79.7% of all reported vulnerabilities. In terms of the amount of leaked information, the websites of financial industry (2.21 billion) and communication operators (1.89 billion) leaked the most information, far higher than other industries. The Internet Society of China issued "*Investigation Report on the*

Protection of Chinese Netizens' Rights and Interests (2016)" showed that 54% of Chinese netizens thought that their personal information was leaked seriously, and 21% thought that their personal information was leaked very seriously. 84% of the people in China personally felt the negative impacts of personal information leakage. On the basis of survey of the report, the leakage of personal information leads to the spread of spam information and rampancy of illegal fraud. Criminals will even use the massive data information that has been leaked to conduct association analysis, and even make user portraits to accurately locate the user's identity and implement accurate fraud. According to estimates, the total economic loss suffered by Chinese netizens each year exceeds RMB 90 billion.

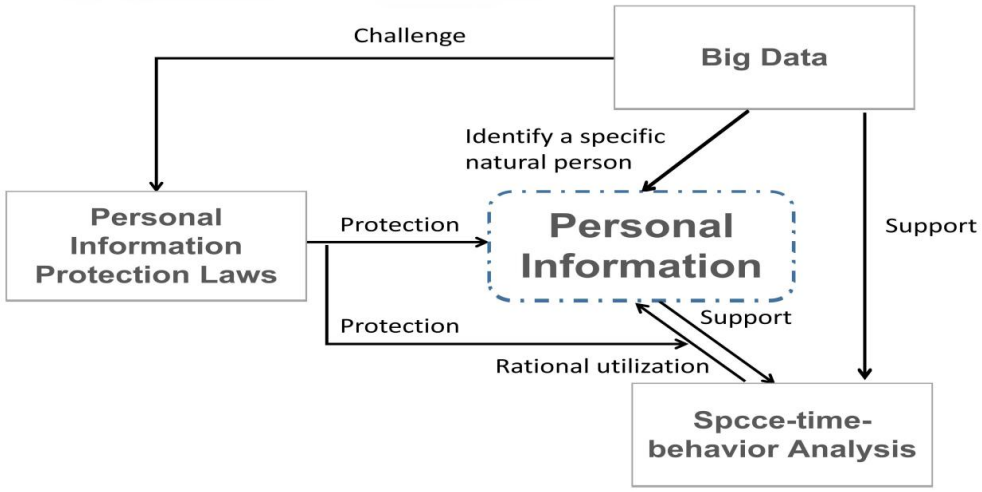


Figure 1-2 Logic relation diagram of background

Informed consent principle, the basic principle of personal information protection, is facing great challenges in the era of big data. How to use personal information legally and rationally, not only to protect personal information security, but also to meet the demands of digital economic development and social public interest, has become an important issue that we are facing. We believe that we should not only protect personal information, but also protect the rational utilization of personal information.(As shown in Figure 1-2) The key to protecting personal information is to protect the core interests of personal dignity and freedom. While the general personal information should be used rationally under the guidance of legal rules.The rational utilization of personal information shall be based on lawfulness,

justification and necessity, and shall not be excessively processed.[①] Legitimacy is the premise and bottom line of the rational utilization of personal information. Rationality is mainly related to the balance of interests of the relevant stakeholders and the maximization of the overall interests under the premise of protecting the core interests of information subjects. Of course, who can get benefit from the "rational utilization", which would be different in various fields of utilization. Therefore, we should follow the rule of rational expectation to evaluate the risk of using personal information in a specific context. The framework of this research work is shown in Figure 1-3.

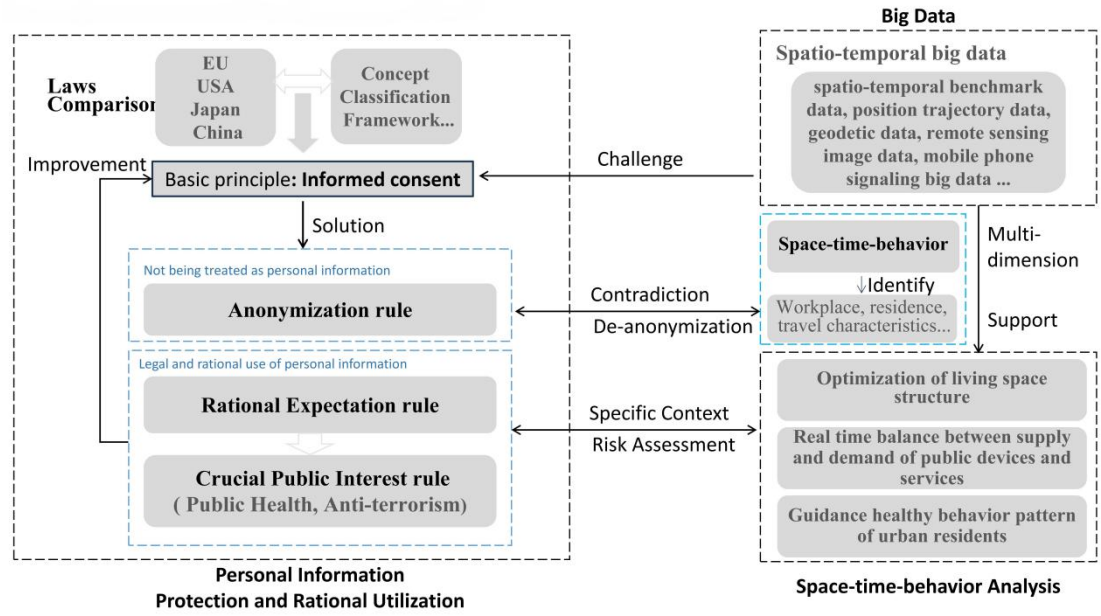


Figure 1-3 Framework of research work

1.2 Literature review

In recent years, many researchers use planning technology and spatio-temporal big data, especially mobile phone signaling big data, to make dynamic analysis of urban spatial-temporal system, and study the characteristics of urban layout, function and human behavior. Shen and Li (2018) expounded how big data can change the ideas of planners and researchers in smart city planning and management practice. Niu, Wang, et al. (2017) proposed a method to measure the hierarchical structure of urban system by obtaining the connection flow between cities from mobile phone signaling big data. ZHAO, HU, et al. (2019) and WANG, GU, et al. (2018) used

① *Civil Code of the People's Republic of China*, Article 1035; *Amended Act on the Protection of Personal Information* (Japan, 2016), Article 15-19.

mobile phone signaling big data to identify the space scale of urban agglomerations and metropolitan areas. It also be used to study urban space structure (NIU, DING, et al., 2014) , identify urban land function (Jin, Chen, et al., 2018), and assess urban construction environment (WANG, ZHONG, et al., 2015). Using the behavior attributes of people reflected by mobile phone signaling big data, Carlo, Dennis, et al. (2006) and Manfredini, Pucci, et al. (2014) studied the intensity changes of urban activities. At the micro scale, it is also used to study the spatial characteristics of urban activities and community differentiation (Yan, Li, et al., 2018), distribution of residents (Becker, Caceres, et al., 2011) and relation between work-place and residence (Zhang, 2016. and Yang, Zhou, et al., 2019), as well as street vitality (Long and Zhou, 2016) and travel characteristics (Lu, Long, et al., 2019 and Yuan, Raubal, et al., 2012) in urban planning and management. By constructing the dynamic analysis framework of population-time-behavior about population distribution, Zhong, Wang, et al. (2017) use it to mine the spatio-temporal features of behavior track, and identify the dynamic features of residents' activities, such as life, work and entertainment.

In the wake of the development about mobile telecommunication and position aware technologies, more and more trajectory data are produced. Mining and using these data can bring people more public services and life convenience. However, trajectory data contains a lot of personal information, such as user's home address, behavior preference, health status and so on. If the location and trajectory data are directly published, people's privacy will be leaked (Wernke, Skvortsov, et al., 2014). Personal information protection mainly considers the followings: (i) how to ensure that the personal information is not disclosed in the process of data application; (ii) how to be more conducive to the application of data. That is, to design personal information protection and utilization path to realize a better balance. CHEN, FUNG, et al (2013) proposed selective suppression of sensitive or frequently accessed locations in published trajectory data, which is easy to implement, but also leads to information loss and limited data availability. ZHANG, MA, et al (2017) added a certain number of false tracks to the original track to make the original track data disturbed and reduce the probability of leakage of the original track. This method is relatively simple, but we should pay attention to ensure the statistical availability of the original track data, and meet the moving state of the false track is similar to the real track. Xiao and Xiong (2015) proposed a differential personal information protection technology based on "δ location set", and advanced a new function

sensitivity measurement method and an effective location perturbation mechanism, which achieves the purpose of privacy protection by hiding the sensitive locations in the location set. This method has a high degree of privacy protection, but the information loss is relatively large, and the availability is relatively low. The most popular method of trajectory privacy protection based on generalization is trajectory k-anonymity, which is to find k similar tracks to construct an anonymous set, so that the probability of the attacker identifying the user's identity without other background knowledge is not more than 1/k (Abul, Bonchi, et al., 2010). Nergiz, Atzori, et al. (2009) generalized the time and space of trajectory data set, uses log cost distance as a measure to judge the similarity of trajectories, and then randomly selects the sampling points in each anonymous region to reorganize trajectories, so as to improve the utilization efficiency of published trajectory data. Yu, Xie, et al. (2017) put forward a technology based on Adaptive Clustering for the issue of dynamic trajectory data release, which can process the real-time trajectory data and segment the trajectory, so that the k-anonymity between every two generalized regions can be satisfied. The above k-anonymity research methods ignore the road network restrictive conditions, and the constructed anonymity sets are not under the road network constraints. Dong and Pi (2018) developed the use of frequent path pattern for trajectory privacy protection, and put forward a personal information protection technology based on frequent path in road network environment. The trajectory was divided into several sections, the infrequent sections were removed, and the most frequent sections were analyzed through a new algorithm to construct the k-anonymity set. This method satisfies the road network constraints and avoids the path reasoning attack.

For de-anonymization of trajectory data, attackers mainly calculate the similarity between the existing information and each user's information in the data set to be attacked, and then selects the one with the highest similarity as the possible result (Narayanan and Shmatikov, 2008). If an attacker obtains some trace fragments of the target in the current or future arbitrary period, the attacker can identify the historical trace of the attacker by comparing the anonymous historical trace data set. The historical track and the trace fragments obtained by the attacker are matched to identify the historical track with the highest similarity with the trajectory features held by the attacker. Zhong, Chang, et al. (2016) and Chen, Zhang, et al. (2017) proposed a novel de-anonymization method, which uses the density-based clustering algorithm to obtain hidden states of HMM from spatio-temporal points of trajectories, and provides

much better performance. This method also add a special model to distinguish the attack process between open context and non-open context. Moreover, the existing patents also show that there are many de-anonymization technologies related to mobile phone signaling big data.

Many scholars have conducted researches on protection and utilization of personal information from various perspectives. From the viewpoint of the definition of personal information, Liu (2017) pointed out that all rational means possible to be taken by controller or third-party user of personal information under the conditions at that time should be considered to judge whether the information was identifiable; Hon, Millard, et al. (2011) believed that when processing information for special purposes, non-personal information might also be transformed into personal information; Xavier (2015) put forward that the analysis and discussion irrelevant to objective state of a person was meaningless for identifying the person and thus didn't belong to personal information. From the perspective of the attribute of right for personal information, people have different understandings of the core interests under the information protection law due to the different legal cultures and social backgrounds of different countries (BOSHE, 2015). Yang (2016) reckoned that personal information had connotations of both spiritual personality interests and property interests, but the attribute of personality right was the essential attribute of personal information; Long (2017) thought that a new kind of data property right should be constructed, based on distinguishing data assets and personal information; Xiang (2018) proposed that personal information property right should be independently confirmed, exercised, and protected, and efficiently configured by market; regarding the public and social natures of personal information, Gao (2018) brought forward the "social cybernetics" of personal information which argued that personal information right no longer only appears as an absolute property right or personality right. From the model of personal information protection, Daniel and John (2007) raised a differentiated privacy protection strategy which provided customized privacy levels for users' personal information and measured the value of privacy; Lv (2021) points out the dilemma and way out of "informed consent" in personal information protection; Tian (2018) held that prior informed consent should be transformed into hierarchical consent on the basis of information classification and context-based risk assessment, and one-time consent should be changed into continuous information disclosure and dynamic consent; Ding (2018) presented that

the rationality of personal information circulation should be judged in specific context and community; Yin and Wang (2016) stated that it is important to establish integrated personal data traceability management system to protect personal information; Sun (2016) suggested that a tort law system with the ultimate user of information as the responsible person should be constructed, orienting to secondary dissemination and utilization of information; Svantsson (2018) studied the complicated relations of data protection laws and consumer protection laws, and claimed to a third-party controller for liability compensation based on data protection as per consumer protection law; Pearce (2017) explored the possibility and feasibility of making interdisciplinary research on personal information protection and risk management; Fan (2016) put forward some concepts based on data context and risk management which provided a new path for the innovation in model of personal information protection.

1.3 Research purpose

In recent years, people have left a lot of data which associated with individuals in the process of receiving smart service. When these data are mined and used by various stakeholders, it may lead to the leakage or abuse of personal information. Therefore, smart devices and smart services not only bring convenience and efficiency to our living, but also bring risks of personal privacy and property due to the collection, sharing and use of personal information. At present, the issue of personal information protection has aroused widespread concern.

Up to now, few studies have discussed the application of big data in space-time-behavior analysis from the perspective of the balance between personal information protection and rational utilization. This research focuses on the protection and rational use of personal information in space-time-behavior analysis based on big data. Through this research, we try to build effective legal rules and judgment standards to realize the balance between protection and rational utilization of personal information. That is, we should achieve not only the protection of personal information but also the protection of rational utilization of personal information. The specific objectives are as follows:

1. To analyse the the basic principle of personal information protection as well as the difficulties it faces through the comparison of the laws of personal information

protection in different countries.

2. To reveal anonymization rule in use is not suitable for the sharing of spatio-temporal big data in space-time-behavior analysis, through the study on the utilization of mobile phone signaling big data.

3. To construct the judgment standard of rational expectation through the risk assessment in the specific application context to meet the interests of different Stakeholders and realize the balance of protection and rational utilization of personal information.

4. To discuss how to make rational utilization of personal information to balance the needs of teaching devices and services during COVID-19 pandemic, and guide students to form good learning behavior and healthy life behavior, to ensure the quality of education and management.

1.4 Research object

In this dissertation, we take spatio-temporal big data, especially mobile phone signaling big data, as the research object. Research shows that mobile phone signaling big data is one of the most commonly used data sources for urban planning in China.

Spatio-temporal big data refers to the big data created based on a unified spacet-ime benchmark. It moves and changes in time benchmark system and space benchmark system, and directly or indirectly related to an specific location (fixed or spatial distribution). (Wang, Wu, et al., 2017) Spatiotemporal big data is a very important basic big data. The natural resources and spatial geographic information database, macro-economic information database, population information database and legal entity information database constitute China's four basic databases. Spatio-temporal big data has both time dimension and spatial dimension, and also has subject attribute dimension, that is multidimensional dimension information. It is important to clarify that:

(I) Spatial dimension (Si: x_i, y_i, z_i) - 3D spatial position distribution information.

(II) Time dimension (T_i) - Dynamic information over time.

(III) Attribute dimension (D_i) - Various subject attributes information over spatial-temporal.

Also, it is noteworthy that spatio-temporal big data generally includes the following kinds of data. Such as spatio-temporal reference data, remote sensing

picture data, geodetic data, location trace data, location-related spatial media data, etc. (Wang, Wu, et al., 2017) It is also on the basis of unified temporal reference and spatial reference. Therefore, it is more perfect, orderly and structured. The sources of spatio-temporal big data are more orderly, and unlike other data randomly formed, its data value is higher and its applicability is stronger. Spatio-temporal big data is used for describing the state of geomorphic elements and people behavior activities. It can provide a 4D environment composed of time and space, and realizes analysis and decision-making based on unified spatio-temporal system. Taking into consideration the features of visualization, spatio-temporal big data can realize virtual display, which is most in line with the needs of people's perception. It can intuitively provide people with the time identification and spatial distribution of information, so as to better display the results of urban construction under multiple data.

As the control command of mobile telecommunication system, mobile phone signaling guides the cooperative operation of terminal, switching system and transmission system, establishes communication channels among different terminals, controls channel connections and transmits network run command, so as to play a maintenance role for the proper operation of telecommunication system. When the mobile phone is in the state of on or off, making a call, sending a text message or logging in to the Internet, it will communicate with the transmitting base station, and the system will generate signaling data to record the usage status of user. In the meantime, the communication base station also records the location of the mobile phone user in the coverage area, and periodically updates the user's location at a certain time interval to form mobile phone signaling information. For this reason, mobile phone signaling big data is a typical spatio-temporal big data. Under a unified spatio-temporal reference, its movement changes in time-space, and it can reflect positions and habits of users. By mining mobile phone signaling big data, and using the activity trajectory generated by its continuous variations in time and space, we can analyze the composition system and spatial layout of the city and the relationship between its functional areas. It can also study the relationship between residents' acts of work, living, entertainment and time-space locations. This provides a new study approach and technical method in space-time-behavior analysis. In the light of *Civil Code of the People's Republic of China*, personal information refers to "various information recorded electronically or in other forms that can identify a specific natural person separately or in combination with other information, including a

natural person's name, date of birth, identity card number, biological recognition information, address, telephone number, e-mail address, health information, and whereabouts information, among others"[①]. Compared with the law, the features of mobile phone signaling big data in line with the legal definition of personal information, so it is obviously a kind of typical personal information.

According to statistics from the MIIT of China, as of 2018, mobile phone users had approached 1.6 billion, and the mobile phone penetration rate had exceeded 112 units per 100 people. Assuming that each mobile phone can generate an average of 100 signaling data per day for calculation, a city with 1 million people will have more than 1.12 million mobile phones, and more than 112 million mobile phone signaling data will be generated every day. Mobile phone signaling big data covers almost all the people, with the characteristics of volume, velocity and real-time. In particular, compared with other data samples, it is more convenient and cheaper. The Urban Data Party of China hosted the selection activity *"2018' Top 10 Big Data Application Institutions of Planning Industry in China"* and evaluated more than 200 big data-based planning projects submitted by various research institutions. The evaluation results show that the use of mobile phone signaling big data has reached 31%, and it is the most mainstream data source in space-time-behavior analysis. (As shown in Figure 1-4)

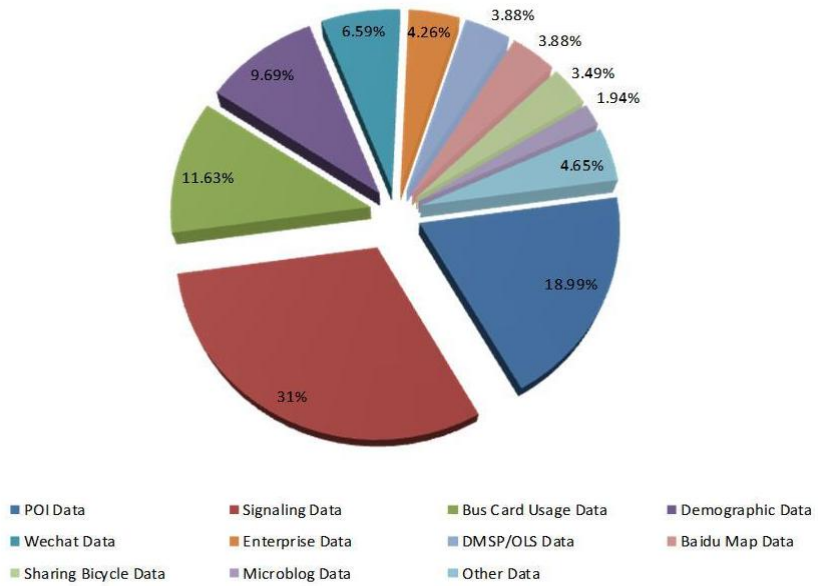


Figure 1-4 Main data sources in space-time-behavior analysis

① *Civil Code of the People's Republic of China (2021),* Article 1034.

1.5 Research approach

First of all, the personal information protection laws and regulations in major countries&regions are collected and compared, and the keyword search is used to investigate the current situation of personal information protection. Through the comparison of legislation frame and supervision mode about protection on personal information worldwide, the basic principle of personal information protection has been discussed. It also analyzes the dilemma of informed consent principle in the era of big data through practical affairs and discusses special rules for personal information utilization.

Then, through patent search and technologies comparison of anonymization and de-anonymization, it is revealed that only anonymous processing of mobile phone signaling big data is used in space-time-behavior analysis, which is not enough to protect personal information. A simple identification method is proposed, that is, matching anonymous trajectory information to the corresponding geographical space, and then marking the active position information in the specific period of time, which can easily identify the key position such as the work-place and residence of users, and even give user portrait.

Next, in order to protect personal information and balancing the interests among stakeholders, the risk assessment model is constructed：

R (I, T, V) =R (P(T, V), S (T, I))

R - Risk of damage to the rights and interests of personal information subject in a specific context

P - Possibility of damage to the rights and interests of personal information subject caused by threat exploiting vulnerability

S - Severity of damage to the rights and interests of personal information subject caused by the threat

I - Interest of personal information subject

T - Threat considering the probability of threat occurrence and its harmfulness

V - Vulnerability according to existing security measures

Through the risk assessment of personal information application in specific context by using matrix method, the rational expectation standard is determined. Taking the application of mobile phone signaling big data in people-oriented urban planning as an example, the combination of quantitative analysis and qualitative analysis to evaluate the risk of personal information sharing in the specific context, so

as to determine whether it meets the "rational expectation" rule.

Finally, through case study, the personal information protection and rational utilization based on crucial public interest during the COVID-19 pandemic in smart campus would be studied.

(As shown in Figure 1-5)

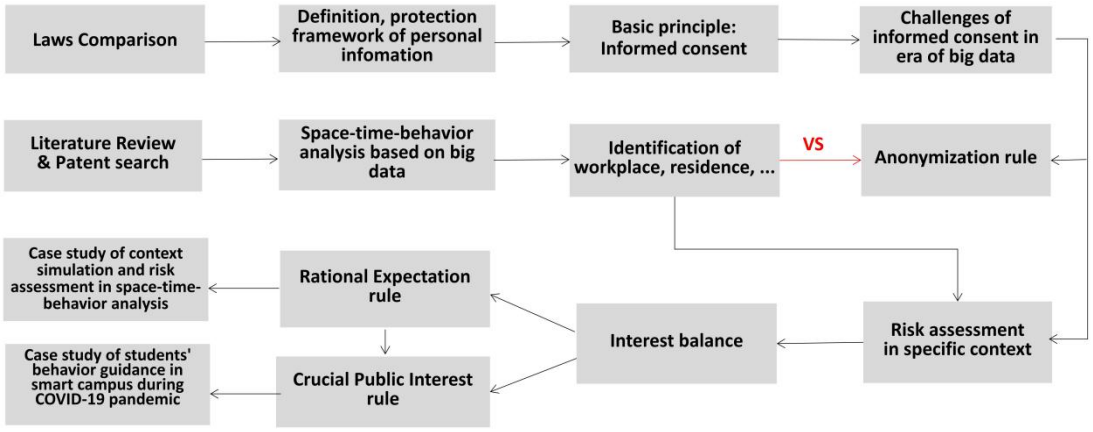


Figure 1-5 Research approach

1.6 Dissertation organization

This dissertation is organized into six chapters as following, in which the second, third, fourth and fifth chapters are the core contents.(As shown in Figure 1-6)

Firstly, in the chapter 1st, the research background, research purpose, research object, research approach and literature review are introduced to support research ideas.

In the chapter 2nd, the concepts about the protection on personal information are discussed, and focuses on the challenges faced by the personal information protection with fast development of information technologies and digital economy. Then, it compares the specific legislative forms and supervision modes of personal information protection around the world, discusses the evolution and current status of personal information protection laws and regulations in Japan and China, and analyzes the commonality of personal information protection and the basic principles of "informed consent". The research shows that information overload, status asymmetry, data explosion and rapid transmission are challenges to the principle of informed consent in the era of big data. Anonymization, rational expectation and public interest use are the rules of personal information protection and reasonable utilization, and are the exceptions of the principle of informed consent. This work has

published in *Proceedings of International Conference 2019 on Spatial Planning and Sustainable Development*, Aug. 30th–Sept. 1st 2019, Chiba University, Japan. (Reference theses ①)

In the chapter 3rd, the anonymization rule of personal information protection in space-time-behavior analysis is studied. In the light of the related laws and regulations, data has been anonymized before being shared, that is, it can not be identified as a specific person and can not be recovered again, will no longer be treated as personal information. In people-oriented urban planning, the mobile phone signaling big data is used for constructing the basic dynamic analysis framework of "space-time-behavior". Even though mobile phone signaling big data is anonymous, it is still inevitable to show some specific position information of users in space-time-behavior analysis. The anonymous trajectory information can be matched to the corresponding geographical space, and then mark the active position information in specific period of time. It can easily identify the specific positions such as work-place and residence of users, and even give users' portraits. Current technologies show that it is easy to be de-anonymized, and anonymization rule is not suitable for personal information protection in space-time-behavior analysis. Mobile phone signaling big data which can reflect the user activity trajectory belongs to sensitive personal information. In case of leakage, it is very likely to invade individual privacy. So, only by using anonymous approach is insufficient to protect personal information security in space-time-behavior analysis, and sharing the mobile phone signaling big data should follow the principle of explicit informed consent or other appropriate rules. This work has been published in *International review for spatial planning and sustainable development*, 2021,Vol. 9(2):76-93. (ESCI, SCOPUS) (Reference theses ③)

In the chapter 4th, the rational expectation rule in specific context is studied. Personal information has the values of personality dignity, economic use and public management. In the age of big data, personal information has been widely shared and used, which facilitates personal life, economic production and social management but also brings the risk of personal information abuse. Meanwhile, the stakeholders relevant to personal information have become more and more diverse, leading to increasingly urgent demand for sharing and using personal information. With the great improvements in the processing efficiency and transmission rate of personal information, it has become much easier to share personal information, which makes the application of the principle of informed consent more difficult. In this

circumstance, "rational expectation" becomes a new option of personal information protection. By assessing the risk of personal information sharing based on application contexts, It discusses in this dissertation the criteria of risk control under rational expectations and puts forward the way to share and use personal information, and to strike a balance among personal information protection, digital economic development and public interest maintenance, so as to drive digital innovation, economic development and social progress, as well as to meet people's requirements, and to effectively protect personal information. This work has been accepted by *International Review for Spatial Planning and Sustainable Development*, Expected January 2022, 20 pages. (ESCI, SCOPUS) (Reference theses ④)

In the chapter 5th, taking Fuzhou University and Kanazawa University as examples, the personal information protection and rational utilization involving crucial public interests in smart campus are studied. By analyzing the notices and policies of Fuzhou University during the COVID-19 pandemic, it studies how universities use personal information rationally to balance the needs of teaching devices and services, guide students' good learning behavior and healthy life behavior, ensure education and management quality during the pandemic. Usually, universities will postpone the opening date of campus and conduct online education when the pandemic is severe, will increase efficiency in campus management and start offline education when the pandemic is slow down. In current online education, the rational use of personal information by universities is insufficient, which affects the quality of teaching. Nevertheless, if the amount of collection and use increases, it will face personal information protection issues. Especially in current offline education, measures taken to prevent and control the pandemic need a lot of personal information, such as travel purpose, health information and so on. For the need of public interest and epidemic prevention, universities can collect and use students' personal information. But it involves personal privacy, it's necessary to increase personal information protection both online and offline education. Through the pilot and questionnaire survey of Kanazawa University, it shows that the more effective application of personal information in online education, and the combination of online and offline education, will greatly help improve the quality of education. Smart campus planning and academic building design should provide more free space suitable for group work to meet the needs of LMS teaching. This work has been published in *Proceedings of International Virtual Conference 2020 on Spatial*

Planning and Sustainable Development, February 6–7th, 2021, https://www.spsdcommunity.org/spsd2020-vc/. (Reference theses ②)

Finally, in the chapter 6th, this dissertation summarizes the conclusions of the doctoral research, puts forward some legislative proposals and points out the limitations of the study and the remains that would be solved in the future.

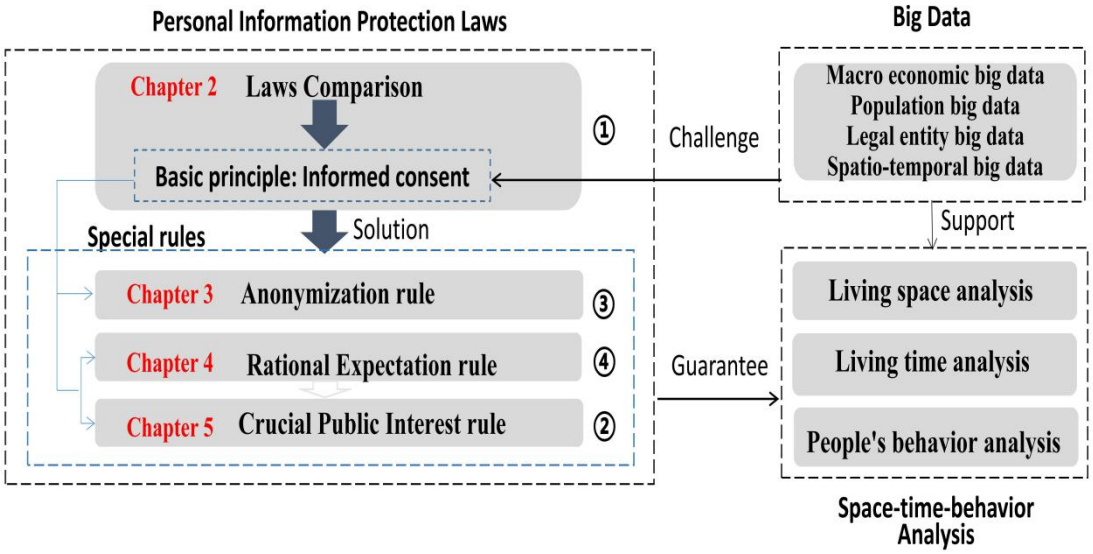


Figure 1-6 Dissertation organization

Chapter 2 Comparative Review on Personal Information Protection Laws in Major Countries

2.1 Introduction

In the era of big data, based on the big data in social network system and geographic information system, smart devices and smart services are bringing us with a new and convenient lifestyle worldwide. (Vandercruysse，Buts, et al., 2020) Most of the big data generated in smart devices and smart services is related to personal information, and it is concerned with the private right and individual safe in public space. Therefore, personal information protection has become an important issue, and it is necessary to clarify how governments and companies that possess smart devices or provide smart services to collect personal information protect personal privacy and security. In the chapter, we study the concept and patterns of personal information protection in different countries, and compare the legislation, supervision and industry norms based on the relevant law system worldwide. Meanwhile, we focus on the comparison between Japan and China for gaining better understanding the legislation actuality in China for personal information protection. Through comparison, the general principle and rules of personal information protection in major countries are obtained, in order to constantly regulate personalized smart services and improve the personal information protection and rational utilization.

By comparing the relevant legislation, we find that the concept of personal information is different from each other in different countries. Regarding the terminology related to personal information that are already widespread, we can find similar terms in other countries such as personal data and personal privacy. In European Union, the concept of personal data is popular. Vandercruysse, Buts, et al. (2020) argued that the enforcement of *General Data Protection Regulation(GDPR)* strengthens the regulatory requirements for data protection of smart services. In common law countries, the concept of personal privacy is more used, and the protection of human dignity and freedom is emphasized.(Brandeis, 2014)

There are some research reports on the current progress of personal information protection in the law system. Raff (2015) said that civil law relief is related to human rights protection, and the private enforcement of competition law is emerging in latter

half of 20th century. Loideain and Adams (2020) studied how to use data protection law to try to solve the societal harm about the role of women. Svantesson (2018) compared the data protection law and consumer protection law, analyzed the relationship between the two laws aiming at different legal relations, and put forward the liability claim based on data protection to the third party non-controller according to the consumer protection law.

There are different law systems in the world, how to deal with personal information protection has different paths. In order to meet the challenges related to personal data protection and coordinate the internal data protection rules, the EU has formulated the *General Data Protection Regulation* (GDPR), which came into effect in May 2018. (Tikkinen-Piri, Rohunen, et al., 2018). Some European countries keep much of their legal system in line with the GDPR of the EU (Ersoy, 2019). In America, Renger, Gotkin, et al. (1998) examined the *Family Privacy Protection Act* of 1995 (FPPA), and studied its potential impact on activities of personal information protection. Machida, Nakamura, et al. (2020) described the changes of personal protection measures implemented by ordinary citizens in Japan from the early stage of COVID-19 epidemic to the stage of community transmission. Chik (2013) introduced the Singapore *Personal Data Protection Act* (PDPA), and evaluated the future trend of data privacy reform according to international privacy standards. Qi, Shao, et al., (2018) explained that China has passed *Cyber security Law*, aimed at strengthening cyberspace governance via corresponding means, such as security protection of Internet operators, special protection of core information infrastructure, personal information protection, data local storage and security assessment of data export.

How to protect the personal information for providing smart services, the legislation work shows available solutions in the form of law and regulation for business model. Mendelson (2017) presented the principles of personal privacy protection that have special patterns and methods to control the ability of third parties in the EU to collect, process and use personal data. Baek, Bae, et al. (2014) reported, as a means of protecting personal privacy, industrialized countries have implemented the legal provisions of informed consent, which means consent of users should be obtained before personal information can be collected. In Japan, Horie, Sasaki, et al. (2006) reported that workers' health information collected by employers is processed according to Personal Information Protection Law. Yu and Zhao (2019) focused on the

development of China's commercial data market, and discussed the issues of personal data rights and data property rights under the background of big data commercial transactions.

Through literature review, we find that the main concern of researchers is that with the rapid advancement of information technology, personal privacy is becoming more and more vulnerable to infringement.(Baek, Bae, et al., 2014) There are more research reports that focus on the information protection rather than the reasonable and efficient use of personal information for smart city services. As the above, there are few researches focus on the comparison of personal information protection and rational utilization in different countries. Especially in the field of smart city planning and management, it is an important topic for improving personal information protection and its reasonable usage in order to provide smart service.

2.2 Research approach

In this chapter, the personal information protection laws and regulations of major countries&regions are collected and compared, and the keyword search is used to investigate the existing circumstances of personal information protection in the age of big data. firstly, the definitions about personal data, personal information and personal privacy are compared in the current law systems worldwide. Next, the legislation frame and supervision mode about protection on personal information worldwide are compared, discussing about the basic principles of personal information protection. Following with comparison between European and American countries, it investigates the historical evolution and current situation of personal information protection law and regulations in China and Japan respectively. Finally, it analyzes the dilemma of the principle of informed consent in the age of big data through practical affairs and discusses special rules for personal information utilization.

2.3 Personal information in the era of Big Data

2.3.1 Overview on personal information

The concept of personal information was sourced from personal "data protection" as proposed in the *Teheran Declaration* at the "International Conference on Human Rights" of the United Nations in 1968. With the advancement in science

and the development of society, especially after entering the age of big data, the amount of data generated annually around the world has increased in geometric progression, so the intension and extension of personal information have also been continuously deepened and expanded accordingly. At present, the legislation of all countries in the world mainly applies three concepts: personal data, personal privacy, as well as personal information.(As shown in Table 2-1)

The legislation with the title of "personal data" mainly includes the member states of EU and the mainly affected countries, such as Germany *Federal Data Protection Act* in 1977, French *Data Protection Act* in 1978, as well as *General Data Protection Regulation* (GDPR) passed by the EU in 2016. The legislation with the title of "personal privacy" mainly includes the common law states, such as American *Privacy Act* in 1974, Canadian *Privacy Act* in 1987, as well as the Australian *Privacy Act* in 1988. The legislation with the title of "personal information" includes *Information Protection Act of Austria* in 1978, *Protection Act on Personal Information of Public Institution* issued by the South Korea in 1999, as well as *Information, Informatization and Information Protection Law of the Russian Federation* issued by Russia in 1999. There are also the examples of the countries who commonly applied personal information and personal data, such as *Protection Act on Personal Information* implemented by Japan in 2005. *Guidelines on Privacy Protection and Cross-border Circulation of Personal Data* passed by board of directors of Organization for Economic Co-operation and Development (OECD) in 1980 simultaneously used two concepts including "privacy" and "personal data". Although China has not yet enacted specific legislation on personal information protection, in the existing legal system, there are already many laws concerning personal information protection, such as the *Civil Code* (2021) and the *Cyber Security Law* (2016), all of which are Use the concept of "personal information". In 2010, *Personal Information Protection Act* issued in Taiwan area applied "personal data" to define the personal information. While the *Personal Data (Privacy) Regulations* implemented in Hong Kong region summarized personal information with data and privacy.

Table 2-1 Origins and countries using personal data, personal privacy as well as personal information

Concept used for legislation	Legal regulations
Personal data	In 1977, Germany *Federal Data Protection Act* In 1978, French *Data Protection Act* In 2016, European Union *General Data Protection Regulation (GDPR)*
Personal privacy	In 1974, United States *Privacy Right Act* In 1987, Canada *Privacy Right Act* In 1988, Australia *Privacy Right Act*
Personal information	In 1978, Austria *Information Protection Act* In 1999, Korea *Protection Act on Personal Information of Public Institutions* In 1999, Russian Federation *Information, Informatization and Information Protection Act* In 2016, China *Cyber Security Law*
Personal information and personal data	In 2005, Japan *Protection Act on Personal Information* implemented

2.3.2 Concept and features of personal information

Personal information is generally defined by "identification theory" in the international community (Qi and Zhang, 2018), namely whether a specific natural person can be identified alone or in combination with other information is used as the core criterion for determining personal information.（As shown in Table 2-2）

Table 2-2 Comparison of personal information related concepts in EU, USA, Japan and China

	European Union *GDPR*	The United States *Privacy Act*	Japan *Amended Act on the Protection of Personal Information*	China *Cyber Security Law*
Legal terms	Personal data	Privacy	Personal information /Personal data	Personal information
Related definition	Any information relating to an identified or identifiable natural person (an identifiable natural person is one who can be identified, directly or indirectly)	Any item, collection, or grouping of information about an individual that is maintained by an agency	Information relating to a living individual/Personal information constituting a personal information database etc.	All kinds of information recorded by electronic or other means that can identify a specific natural person individually or in combination with other information
Contents (includes, but not limited to the following)	A name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	Education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph	A name, date of birth, race, creed, as well as social status, medical history, criminal record, fact of having suffered damage by a crime, or other descriptions etc. (recorded or otherwise expressed using voice, movement or other methods in a document, drawing or electromagnetic record), an individual identification code	Natural person's name, date of birth, ID number, biometric information, address, telephone number, e-mail, health information, track information, etc

Nowadays, big data based information processing technology has become mature. Followed by, more and more personal information is dug out and used. For enhancing the protection of personal information, whether a type of information belongs to personal information can be judged as per the following three features: The first is identifiability, that is a specific natural person can be identified on the basis of the information alone or in combination with relevant information, such as name,

telephone number, and passport number; The second is idiosyncrasy, which means that the information describes the special personality or state of a given specific natural person, such as personality preferences and health status; The third is correlativity, namely the information reflects the activities of specific natural person, for instance, personal track and network browsing history[①]. The information having any of the said three features should be judged as personal information and thus be protected.

Therefore, personal information refers to the data recorded by electronic or other means, which can identify the identity of a specific natural person alone or in combination with other relevant information, or reflect the personality, statue, behavior of a specific natural person.

2.3.3 Legal analysis of the concepts of personal information, personal data and personal privacy

2.3.3.1 The relationship between personal information and personal data

Personal data is closely related to the concept of personal information. In the legislative practices, the extensions and connotations of both personal information and personal data are almost the same (Tian, 2018). As what mentioned before, the concept of personal data is mostly applied by the member states of European Union and most of other countries who are influenced by European Union Personal Data Protection Directive in 1995 thus to make legislation. In the countries such as Korea, Russia and China, the concept of "Personal Information" is applied. Therefore, understanding from the relatively unified concept, the basic connotation of two concepts including personal information and personal data is the same, and the difference is about the expression.

Japan makes a distinction between personal information and personal data in the *Personal Information Protection Act,* and introduces the concept of personal information database: "A collective body of information comprising personal information, including those systematically organized so as to be able to search for

① *Consumer Privacy Bill of Rights Act（Draft）（USA，2015）*

particular personal information using a computer and those prescribed by cabinet order as having been systematically organized so as to be able to easily search for particular personal information". Personal information in this Act means that "information relating to a living individual" and personal data in this Act means "personal information constituting a personal information database etc". According to this definition, it can be considered that personal data is structured and easy to retrieve personal information which is processed and organized according to certain rules. Objectively, all data collection should be based on certain rules. There is no clear boundary between processing data and original data. The difference between personal data and personal information is mainly based on the needs of specific legislation.

2.3.3.2 The relationship between personal information and personal privacy

The other concept which has lots of superposition with personal information in terms of contents is personal privacy. In the common law countries, such as the United States, Australia, Canada, as well as New Zealand, and the Asia-Pacific Economic Cooperation (APEC) which is greatly influence by the United States, the concept of personal privacy is most frequently applied. The so-called privacy right is usually referred to the right that the private life is not intervened, or the right that personal privacy cannot be opened without permissions.(Brandeis, 2014) That is to say, everyone has the right that not disturbed and intervened by others. Personal privacy right mainly aims at protecting personal life to be quiet and private. The essence of privacy right is that the individuals can determine when and where to communicate with the outside world at what kinds of modes.

From the perspective of concept, it is generally believed that personal information and personal privacy are different to some extent, and there is an inclusive relationship between them. Personal information covers personal privacy, and personal privacy is a subset of personal information. From the connotation and extension of the two concepts, a considerable part of personal information beyond the scope of privacy. A typical example is the information that is publicly known within a certain time and space with the consent of the information subject, such as personal name, work unit, telephone number and so on. Because it no longer has privacy

attributes, it has nothing to do with personal privacy, but undoubtedly belongs to the scope of personal information. From the perspective of their value orientation, the protection of personal privacy focuses on preventing personal privacy from being illegally disclosed, maintaining the peace of private life, and protecting the right and interest of personality. On the contrary, the value basis of personal information protection is the independent control and active use of personal information, and its focus is to protect the self-determination right of personal information, which is not only the independent control and disposal of personality rights and interests, but also may involve property rights and interests.

However, from the perspective of right, there is a certain crossover between information right and personal privacy right, both them are one of the right of personality. On one hand, lots of unopened personal information belongs to the category of privacy. In fact, lots of personal information are the private information that people are not willing to open to the outside world, and are the private spaces that individuals do not want others to intervene in. No matter they have the economic value, they all show a personality benefit. On the other hand, parts of privacy rights protecting the objects also belong to the category of personal information. Especially that we should see that the development of digitalization technology makes lots of privacies possess the characteristics of personal information at the same time, such as personal communication, these all can be processed by technology and be digitized thus to be further included into the category of personal information.

2.3.4 Classification of personal information

2.3.4.1 Classified by personal information content

Personal information can be divided into personal identity information, personal biometric information, personal physical health information, personal resume information, personal property information, personal network identity information, personal social network information, personal communication information, personal Internet use record information, personal smart equipment information, personal location and track information, As well as religious beliefs, sexual orientation,

undisclosed criminal records and other kinds of information. (As shown in Figure 2-1)

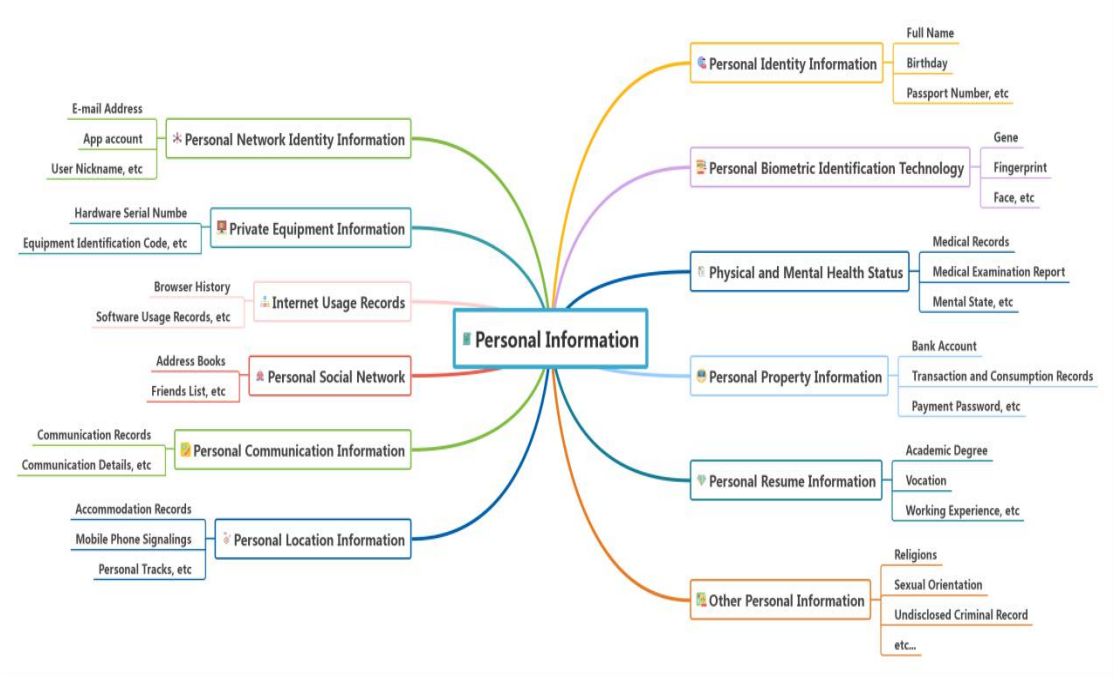


Figure 2-1 Classification of personal information by content

2.3.4.2 Classified by personal information sensitivity

General Data Protection Regulation (2018) adds the concept of "sensitive data", and *California Consumer Privacy Act of 2018* gets personal information divided into general personal information and sensitive personal information as per the sensitive attributes of the information. In *Amended Act on the Protection of Personal Information* (Japan), it is called "special care required personal information". As stated in the *GDPR (2018)* of European Union, sensitive information includes the personal data revealing one's race or ethnicity, political opinions, religious or philosophical beliefs and union membership, as well as the gene data for unique identification of natural person, the biometric data, health data, and sexual life or sexual preference. In the national standard of China, *Information security technology: Personal information security specification* (GBT 35273-2020), sensitive personal information is defined as the information that may endanger personal and property safety and is easy to lead to damages or discriminatory treatment of personal reputation and physical and mental health once being disclosed, illegally provided or abused. It generally involves a person's biometric information, physiological health

information, bank account and payment information, transaction and consumption record, communication log and content, track, accommodation information, sexual preference, religious beliefs, undisclosed criminal record, as well as personal information of children not older than 14 years old. The cognition of sensitive information varies in different country and different society, and is affected by many factors including the sense of values, religious beliefs, cultural customs, and the comprehensive extent of legal system (BOSHE, 2015). Nevertheless, the information involving personal privacy should be generally classified as sensitive personal information.

2.4 Personal information protection in major countries

In 1970, the first personal data protection law in the world was enacted in Hessen, Germany, and hence, major countries in the world established their own legal system in terms of protection on personal information in succession. In Table 2-3, we make a comparative review between EU, USA, Japan and China for getting better understanding of the framework of personal information protection in major countries.

2.4.1 Legislation model in United States and European Union

Personal information protection legislation, the United States and the European Union as typical representatives.

The United States is the mode combining scattered legislation and industrial self-discipline, and it takes privacy right and freedom as the foundation of constitution and administrative law. In the public field, the scattered legislation is adopted for legislation one by one. In the private field, the United States depends on the self-discipline mechanism including corporate standard of behavior, folk certification system as well as alternative dispute solution mechanism. In the light of the specific contents of personal information, the corresponding supervision department takes charge of supervision to realize the protection on personal information. The *California Consumer Privacy Act of 2018* (CCPA) has come into effect on January 1, 2020, and has become the most influential data privacy legislation at state level in the United States. There are also strict legislations in various industries, such as *Fair*

Credit Reporting Act (FCRA) in the field of finance, *Family Educational Rights and Privacy Act* (FERPA) in the field of education, *Health Insurance Portability and Accountability* (HIPPA) in the field of health care, *Children's Online Privacy Protection Act* (COPPA) in the field of children's privacy, etc.

The European Union follows a unified legislative model. In 1970, the first personal data protection law in the world was enacted in Hessen, Germany, and hence, all countries in Europe established their own legal system in terms of protection on personal information in succession. However, because different countries have different laws, there was not unified process modes on personal information processing and protection on personal privacy among member states of European Union. Therefore, in 1995, the EU passed the classical *Personal Data Protection Regulation*, and this legislation of protection on personal information implemented in the whole Europe involves into a huge scope with clear execution mechanism. The European Union mode can also be called as the unified legislation mode, and namely, formulating a comprehensive protection act on personal information to stipulate the collection, processing and utilization of personal information, this act is uniformly suitable for public departments and non-public departments, and moreover, it sets up a general supervision department for centralized supervisory. The EU makes Europe become the model of global protection on personal information in terms of information protection in virtue of this law. In 2016, the EU passed through the revised act *General Data Protection Regulation* (GDPR), its major purpose also includes the management method of optimizing data to flow to the countries outside European Union, and enhancing users' control on their personal information.

The European Union regards personal information as a part of the citizen personality and human rights. The United States regards personal information as a part of the citizen privacy and freedom. We take *GDPR* and *CCPA* as examples to compare and analyze the two legislative models:

(1) Jurisdiction. *GDPR* has a wide range of jurisdiction and complicated logic. As long as it is related to the EU, EU residents, exporting products and services to the EU or monitoring EU individuals, it generally belongs to the jurisdiction of *GDPR*.

On the contrary, the jurisdiction of *CCPA* focuses on enterprises that process personal information for profit, sets the annual income threshold, and focuses on the jurisdiction of entities with large risk impact and scope, so the law enforcement is more targeted.

(2) Personal information cross-border transmission control. *GDPR* is strictly restricted and restrictions are set: The white list of adequacy decision; Whether appropriate agreements and codes of conduct are provided to guarantee cross-border transmission; Group internal rules and approved by regulatory authorities; Passed the necessity test and accidental judgment, etc. *CCPA* is more tolerant of cross-border transmission, although there are some restrictions, but it encourages cross-border data flow and utilization from the perspective of value orientation.

(3) Personal information processing rules. *GDPR* stipulates that the personal data processing is prohibited in principle and allowed when there is legal authorization, and individuals have the right to object to or withdraw authorization; *CCPA* is allowed in principle and prohibited conditionally. *GDPR* is based on the position of regulators, taking the protection of basic human rights as the starting point, emphasizing that data controllers actively regulate the behavior of data processing; *CCPA* is more inclined to the position of data users, focusing on regulating the rational utilization of data.

In summary, the European Union pays more attention to the basic rights and interests of data, while the United States emphasizes the free market model based on strong supervision. On the surface, the two models of the EU and the U.S. are incompatible with each other, but in fact they share the same goal. They both seek a balance between data rights protection and data free flow. The EU model is biased towards the "data rights protection" side, which aims to create the basic data rights of citizens; However, the U.S. model is inclined to the "free flow of data" side, which aims at the development of digital economy. We believe that the protection of personal information rights is conducive to the development of digital economy, and the key is to pay attention to the balance between data rights protection and data circulation. In the age of big data, the balance between personal information

protection and the development of digital economy should be a trend of data legislation; Strengthening the self-discipline of the industry, introducing independent third-party institutions for evaluation, and strengthening the supervision of the government at the level of law formulation and implementation should become an effective path for the protection and rational use of personal information.

2.4.2 Framework of personal information protection in EU, USA, Japan and China

As shown in Table 2-3, there are similar framework of the laws and regulations on the protection of personal information in the worldwide.

Among which, Europe, the United States, Japan, and China all stipulated the pattern of personal information protection, scope of utilization, informed consent system, overseas data transmission restrictions, as well as personal rights on data use at different degrees. In which, European GDPR is the strictest in terms of this condition of sharing to the third-party without the permission of the party. It extremely protects the personal benefits but also limits the re-utilization of data within the reasonable scope to a certain degree. Meanwhile, the United States values industry self-discipline and participation of mass organization, thus to form the unique mode of protection on personal information. Japan established the anonymous processing system of personal information utilization earlier. When anonymous processing via data can protect personal information, the new business mode can be created in the field as smart services in the future via analysis of big data.

Table 2-3 Comparison of the framework of laws and regulations contents related to personal information in EU, USA, Japan and China

	European Union *GDPR*	The United States *Privacy Act*（*Including Amendments*）	Japan *Amended Act on the Protection of Personal Information*	China *Cyber Security Law*
Utilization scope	Scope of use consented by the party (opt in) or public interests	Scope of use consented by the party (opt out)	Scope of use consented by the party (opt out/opt in according to information sensitivity)	Scope of use explicit consented by the party (opt in)

Supervision organization	European commission for data protection	Federal Trade Commission (FTC)	Personal information protection council	Cyberspace administration of China
Provide to the third party without the permission of the party	Not allowed	Not allowed, except de-identified data (unrecognized data)	Not allowed, or allowed after anonymously processing except the personal identification symbol	Not allowed, except specific individuals cannot be identified after processing and are not recoverable
Cross-border transform of data	Limitation	Limitation	Limitation	Limitation
The party's scope of rights towards personal information	Right to know, right to access, right to rectification, right to erasure, (right to be forgotten) right to restriction of processing, right to data portability, right to object	Right to determine, right to access, right to prevent, right to correct or amend, right to withdrawal, right to elimination	Right to know, right to correction, addition or deletion, right to utilization cease or deletion	Right to know, rights to delete, right to correct, right to consent, right to access, right to cancel, right to withdraw
Change of use purpose	Not allowed	Opt in allowed	A reasonable range associated with the pre-change utilization purpose is allowed	Opt in allowed

The personal information protection laws and regulations in China is more flexible for big data administration and permission, in the next we will compare the China and Japan for personal information protection.

2.5 Evolution of personal information protection legislation in Japan and China

2.5.1 Laws and regulations of personal information protection in Japan

Comparing with China, the protection laws and regulations on personal information in Japan are stipulated with systematic, specific and professional characteristics (as shown in Table 2-4). It sets up the independent supervision and

control institutions, and through constant improvement, it enhanced all kinds of regulations on protection on personal information. Through setting up the characteristic anonymous processing rules, it promoted the commercial development of big data under the premise of better protecting personal privacy.

Table 2-4 Historical changes of personal information protection act in Japan

Legislation time	Legislation content
In 1980	*Guidance on International Circulation on Personal Privacy Protection and Personal Data*
In 1988	*Laws related to the protection of personal information related to the computer processing of administrative organs*
In 2000	*Basic law on the protection of personal informatio*n - Special committee on the legalization of personal information protection
In 2005	*Personal Information Protection Act*
In 2014	*Outline of amendments of use system of personal data*
In 2017	Comprehensive implementation of *Amended Act on the Protection of Personal Information*

The protection act on personal information in Japan was firstly formulated in 2005, and among which, the definitions and concept on personal information are vague and unclear, and moreover, there are no independent supervision institutions. In 2017, it issued and implemented the revised personal information protection act. The major revised contents are shown in Table 2-5.

Table 2-5 Comparison between before improvement and after improvement of personal information protection act in Japan

	Personal Information Protection Act	*Amended Act on the Protection of Personal Information*
Personal information	Name, date of birth and other descriptions refer to the identifying personal information	The same
Personal identification symbol	None	Fingerprint, face recognition, passport number, driver's license number, as well as telephone number
It needs to consider about the personal information	None	Race, creed, social identity, as well as criminal record, etc.
Limitation of users of personal information	Practitioner institutions above 5,000	Unlimited

Provided by the third party	Proved by the party in advance	After anonymous processing, the information provided by a third party cannot be re-identified at the same time
Change of utilization purpose	A rational utilization scope that is strongly related to the purpose of the pre-change use is allowed	A rational utilization scope that is relevant to the purpose of utilization before the change is allowed
Overseas providing	The same with the standard of the providing in domestic	Special conditions for overseas providing
Supervision institution	General secretary, identified group	Personal information committee
Punishment	Administrative sanction	Crime of information providing

The personal information protection act in Japan is revised aiming at the following points:

Definition of the personal information

It increased the definition after modification, the personal identification symbol related to bodies, including the race, creed, and social identity and other information which need to be considered. Personal identification symbol cannot be provided to the third party even after anonymous processing. It needs to consider that personal information must pass through the prior agreement in acquiring and providing.

Different utilization purposes

In the original use of the purpose of the need to have a considerable relevance to the considerable deletion. However, the degree of moderation of the purpose is not clear.

Mechanism moderation when providing to the third party

After eliminating the personal identification information, it passed through anonymous processing, and it can be disclosed to the third-party even without the permission of the party. However, it must guarantee that the data won't be able to conduct the re-recognition of personal information.

Overseas providing system

Before the act is amended, it didn't clearly stipulate whether it can conduct the data overseas providing. After the act is amended, it can be provided to outside organizations and countries with the prior agreement.

Supervision organs

After the act is amended, it set up the personal information protection council, which can check and guide the standard of anonymous processing information and companies related to personal information.

Relevant penalties

After the act is amended, the act newly adds the crime of providing data, and within the legal scope, it clearly stipulated the penalty rules.

Among which, anonymous processing information eliminated the changes on the point that the personal re-recognition information can be shared to the third-party without permission, and therefore, it can better utilize big data when protecting personal information, bringing convenience to people's life and creating more commercial value. At present, big data technology is developing toward the direction of collection, use and storage of the information which doesn't directly connect with users. And therefore, it needs to value more about the end of use of information, and make the informed consent system in Japan more transparent and operable.

2.5.2 Laws and regulations of personal information protection in China

At present, there is no special law on personal information protection has come into force in China.[①] The regulations of personal information protection is composited commonly by some articles of the relevant laws, administrative regulations, local laws and stipulations, all kinds of normative documents as well as department regulations. The *Civil Code*, which just came into effect on January 1st,

① Update: *Personal Information Protection Law of the People's Republic of China*, as adopted at the 30th session of the Standing Committee of the Thirteenth National People's Congress of the People's Republic of China on August 20, 2021, shall come into force on November 1, 2021.

2021, also has some principled provisions on the protection of personal information. The practice time is not long, and therefore, it still doesn't form the system aiming at the legislation on personal information, and they are scatteredly appeared in some cases, with scattered execution situations. Thus comparing with the legislation actuality in Japan, China still has a long way to go.

Constitution

Although China's constitution doesn't clearly stipulate the personal information, in the article 38 of China's *Constitution*, it stipulates "the personal dignity of citizens is inviolable". The above text analyzes that personal information right possesses the property of right of personality, and therefore, this stipulation can be regarded as the source of protection of personal information right. Meanwhile, in the *Constitution*, the article 39 and 40 stipulated that "citizens' homes shall be inviolable and unlawful searches shall be prohibited" and "the freedom and privacy of citizens to communicate shall be protected by law", which can also be regarded as the protection on citizens' personal information right.

Laws

In the *Civil Code*, the article 1032 stipulates "A natural person enjoys the right of privacy. No organization or individual may infringe upon any other's right of privacy by spying, intrusion, divulgence, public disclosure, or any other means". And the article 1034 stipulates "The personal information of natural persons is protected by law". As well as the article 1034 to 1039, the definition of personal information, the principle of dealing with personal information, the rights of information subject and the duty of confidentiality that government agencies and public servants should perform are stipulated. In the *Criminal Law*, the article 245 stipulates the crime of unlawful search of a citizen's residence, and the article 252 stipulates the crime of violating the freedom of communication of citizens. *Amendment to Criminal Law (VII)* increased crime of illegally selling or obtaining citizen information. In the *Cyber security Law*, the article 40 to 50 stipulate that network operators shall keep the

personal information of users collected by them strictly confidential, and establish and perfect the system for the protection of users' information. In Law of the *People's Republic of China on the Protection of Minors*, the article 30 stipulates that juveniles' privacy shall not be disclosed. In *Law of the People's Republic of China on the Protection of Women's Rights and Interests*, the article 42 stipulates that women's personality right is protected by law. In *Law of the People's Republic of China on Resident Identity Cards*, the article 6 stipulates that the public servants shall keep secret for citizens' personal information. In *Statistics Law of the People's Republic of China*, the article 15 stipulates that the private and family investigation data cannot be disclosed without the permission of the individual and family. The above can all be regarded as the protection on the citizens' personal information rights.

Administrative regulations and Provisions

At the present stage of China, the relevant administrative regulations and provisions also make specific stipulation on personal information protection from different management perspectives. Such as *Provisions on Protecting the Personal Information of Telecommunications and Internet Users, Provisions on the Cyber Protection of Children's Personal Information, Regulation of Issuing the Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations.*

others

Furthermore, China legislature has passed some personal information protection decisions, which also have certain legal effects. Such as *Decision on Strengthening Information Protection on Networks*, aiming at "protecting the security of network information, maintaining the legitimate rights and interests of citizens, legal persons and other organizations, and safeguarding the national security and public interest".

In addition, the National Standardization Management Committee has also formulated some guiding standards to regulate the protection of personal information. Such as *Information security technology: Personal information security specification (GBT 35273-2020)*.

The above legal provisions are the protection situation on citizens' personal information right in China at present. The legislative evolution and main laws and regulations are shown in Table 2-6. It can be seen that at present, China's clauses about legal protection on citizens' information right are scattered, without a system. Up to present, China doesn't have the special law and protection institution aiming at citizens' personal information right.

Table 2-6 Relevant laws and regulations on personal information protection in China

Legislation time	Legislation contents
In 2009	In *Amendment to Criminal Law (VII),* the article 7 stipulates the crimes on personal information
In 2012	*Decision on Strengthening the Protection of Network Information* firstly established network information rule at the legal level
In 2015	The added article 286 in *Amendment to Criminal Law (IX)* clearly stipulates the harmful consequences caused by network service provider who do not perform the network security management obligation and constituting a crime.
In 2016	Standing Committee of the National People's Congress passed *Cyber Security Law of the People's Republic of China*, and further clearly stipulated the cyberspace users' personal information security
In 2017	*Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Infringing on Citizens' Personal Information,* to further explain the application of law in criminal cases of infringement of personal information
In 2020	The National People's Congress formulated the *Civil Code* of PRC, which has made more complete legal provisions on the right of privacy and the protection of personal information

2.6 Basic principle of personal information protection

2.6.1 General protection mode based on informed consent principle

The principle of informed consent refers to the collection, utilization and sharing of personal information must be based on the premise of fully informing the information subject and with his own (or guardian) true consent. The concept of informed consent originated from Westin (1967), who proposed that individuals have the right to decide when, how and to what extent to transmit their own information to others. In 1980, the OECD issued the *Guidelines on the Protection of Privacy and*

Transborder Flows of Personal Data, which stipulated that the collection of personal data must be legal and fair, and obtain the consent of the party. This criterion has laid the foundation of early personal information protection in the world. Now, it is a basic principle for personal information protection, and also the most basic applicable rule for data collection and utilization.[①] The principle of informed consent includes two meanings: one is "informed", that is, the information subject's understanding of the personal information that the information collector will or has collected and used; The second is "consent", that is, the information subject's permission to the information collector's behavior. Consent must be true, and there is no risk of coercion or fraud. Consent also must be specific, and general consent without definite purpose is invalid. In particular, consent to sensitive information should be explicit. The principle of informed consent aims to protect the information self-determination of individuals. Personality right and interest are exclusive. The legal premise of information collection, utilization and sharing is to obtain the consent of information subject, which needs to inform to the information subject, so that the information subject can know the existence and use status of its own information, and avoid the harm caused by information asymmetry. Therefore, the focus of this process is "consent". "Informed" is the premise and basis of "consent", and consent is the core and purpose, which is the expression of intention that the information subject decides whether his information is used or not. In principle, the informed consent of the information subject should be obtained when collecting, using and sharing personal information.

2.6.2 Dilemmas of the principle of informed consent

As mentioned above, informed consent is the general principle of personal information protection law in the world. Its purpose is to require personal information processors to perform the obligation of informing before processing personal information, so as to balance the information processors who are in a strong position due to information asymmetry and protect the legitimate right and interest of personal information subject. In practice, information processors usually fulfill the obligation

① *The Privacy Act(USA)；The General Data Protection Regulation (EU)；Civil Code of the People's Republic of China.*

of informing through privacy policy or personal information protection policy, and give individuals the opportunity to click to agree. However, in the age of big data, the principle of informed consent also faces many challenges, and may even lead to the failure of the personal information protection mechanism based on this framework. Professor Solove (2013) first proposed the "informed consent dilemma" to describe the situation where the principle of informed consent failed in the practice of handling personal information due to some reasons, thus failing to achieve effective protection of personal information.

2.6.2.1 Information overload lead to inform but unable to know

Under the mechanism of informed consent, if the information processor conceals the behavior of collecting and using personal information, it will face adverse legal consequences. In order to protect themselves to the maximum extent, enterprises have formulated lengthy privacy policy (or personal information protection policy) notification documents. For example, the privacy policy of CMCC, the Chinese mobile communication operator, has 7266 words; Wechat, the most commonly used social and instant messaging software in China, its notification document "Wechat Privacy Protection Guidelines" has 11545 words. The total words in the privacy policy and terms of service of zoom, the conference software we often use, is as high as 14315 words. According to the reading speed of 200 words per minute, it takes at least 30 minutes or even more than an hour to read these notification documents. The length of the notification documents is generally longer and the language is obscure. Obviously, the main purpose of formulating and providing these notification documents is not to promote individual informed consent. The purpose of enterprises performing notification is more to avoid legal risks and seek the maximum legalization possibility for their information processing behavior. This is far from the purpose of establishing the principle of informed consent, which is to protect the right to know and information self-determination of the subject of personal information through notification, resulting in a serious deviation between the purpose of notification and the actual effect. It can be seen that there is a fundamental contradiction between "full notification" and "easy to understand" in personal

information protection policy: Full notification will lead to lengthy content, making users unwilling to invest time in reading and understanding; And easy-to-understand notifications are conducive to users' reading, but it is often difficult to comprehensively convey information protection policies, which exposes information processors to legal risks. (Solove, 2013)

2.6.2.2 In asymmetric status and lack of choice for users

Even if users read the privacy policy carefully, they often lack the space to choose when making licensing decisions, and there is only a state of all or nothing. When users make a decision on whether or not to agree with information processing, it is usually accompanied by the actual demand for the corresponding information network service, and it is difficult for users to make a choice other than consent, unless they give up using the service. Information processors take advantage of this demand that can not be given up and occupy a dominant position in the processing of personal information. For individual users who have no choice, no matter whether they seriously study the privacy policy or not, they can only click "agree". In the long run, users will not seriously study the privacy policy, because it can hardly change the result of choice. Even if the website platform or application software provides the option to modify the default settings of privacy and personal information protection, most users will not spend a lot of energy to do so. After all, most users are not professionals and lack of corresponding legal knowledge. Moreover, in the face of hundreds of applications, it is almost impossible to make appropriate changes to each privacy policy. This is not so much the protection of users' rights and interests as a burden on users.(McDonald and Cranor, 2008) According to the research, users lack effective choice space, but in order to obtain convenient services, they still have to agree to the collection and utilization of personal information, which will lead to users being less sensitive to the consent requests issued by information processors. In most cases, they will click consent directly, which makes the effectiveness of the informed consent rule worse.(Bart, 2014)

2.6.2.3 Data explosion brings more burden to information processors

Big data is rapidly improving the survival and development of human society.

The principle of informed consent for personal information protection, which was established more than 40 years ago[①], inevitably has limitations in its theoretical basis and system design. In the era of big data, the huge amount of data usage makes it costly for information processors to "inform" the information subject, which is lack of feasibility in practical operation. For example, using mobile phone signaling big data for space-time-behavior analysis often requires hundreds of millions of data, involving millions of people. It is difficult for information processors to inform information subjects one by one and obtain informed consent. With the fast development of ICT, IOT, 5G technology, data transmission is more and more convenient, and data sharing is very common in the age of big data. However, when processing the shared data, how to conveniently get the secondary authorization of the information subject is also an objective problem faced by the development of big data industry. The secret of big data analysis lies in that there is no "purpose" before data analysis. Through the analysis of full sample data, we can get the value of data and even the inspiration of data innovation from the correlation between seemingly unrelated things. That is to say, in the era of big data, people's thinking path of using data has undergone a fundamental change. It's often hard to accurately describe the purpose of information processing, which makes it difficult for the information subject to really know.(Mantelero, 2017) For users, under a single information processing purpose, it may be safe to agree to the information processor to use personal information once. But in the age of big data, ubiquitous data collection, accumulation, analysis, and comparison can easily construct a complete personality image of user, and it is very easy to dig out sensitive information that individuals do not want to be known to others, which brings troubles and harms to the information subject. In a word, the batch processing, multi-party sharing and non-specific purpose of massive information increase the difficulty of obtaining effective consent. (Tian, 2018)

In summary, the principle of informed consent aims to change the status

① *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 1980)

asymmetry between the subject and the processor of personal information, and protect the right to know and information self-determination of subject, which constitutes the cornerstone of traditional personal information protection. However, in the age of big data, the informed consent mechanism also faces difficulties in practice, which can not be effectively implemented. Based on the principle of informed consent, different rules are needed as supplementary options to meet the new challenges in the age of big data.

2.6.3 Special rules for personal information utilization

In the age of big data, some special rules are also applied to the collection, processing and sharing of personal information. Especially in some specific contexts, data sharing behavior is hard to obtain the informed consent of personal information subject completely or timely(Zhang, 2020). Therefore, there is a need to strengthen the protection of information subject by using certain specific rules to over the shortage of the principle of informed consent in practice. Generally speaking, there are two main ways. One is to deidentify personal information, so that it's no longer treated as personal information and the object of legal protection. The other is to make the use of personal information is legitimate, rational, necessary and risk controllable through exception rule.(As shown in Figure 2-2)

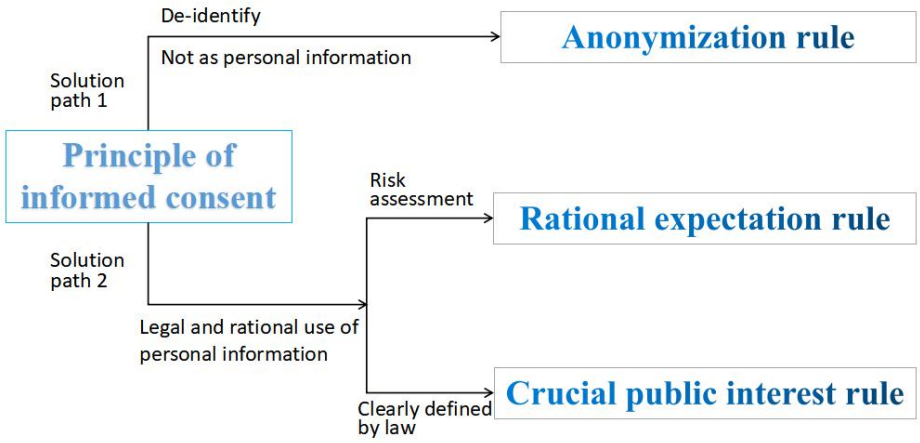


Figure 2-2 Logic relation diagram of background

2.6.3.1 Anonymization rule

Anonymization means the de-identification of personal information. General

speaking, if the information involving individuals is processed anonymously, the contact between the information and the information subject is blocked and cannot be re identified under the existing technical conditions, it is no longer considered personal information. Both Chinese and Japanese laws on information protection have this provision.① After anonymization of personal information, it will be regarded as general data and no longer the protected object of personal information protection law. In this situation, data sharing usually does not require the informed consent of the original information subject.②

2.6.3.2 Rational expectation rule

Under certain conditions, the protection and utilization of personal information should premeditate whether the processing of personal information in specific context conforms to the "rational expectation" of the public.(Wang, 2019) In other words, when personal information is used in a specific context, if the information processing behavior can be expected by the relevant parties, especially the information subject, and this processing behavior can be recognized at the level of general social cognition, then the processing behavior is reasonable, there is no need to obtain the informed consent of information subject. For instance, in China, for the sake of optimizing urban road traffic guidance and achieving timely feedback of traffic information, the government traffic management departments need to set up smart perception devices to collect on-site data of passenger flow and vehicle flow, and then hand it to a professional third-party organization to make real time dynamic traffic guidance. But in this context, people are aware of the data collection behavior, but it is hard to get the consent of the information subject in advance on the technical level. At this point, to determine whether the data collection behavior infringes personal privacy, it should be based on whether the data collector has carried out the necessary risk assessment, whether the collection of information has performed reasonable and careful attention, and whether it is consistent with the general social perception for such behaviors. Hence, in the process of personal information sharing and use, apart from the

① *Civil Code of the People's Republic of China*；*Correction of Prot*ection Act *on Personal Information*（*Japan*）.
② *Civil Code of the People's Republic of China,* Article 1038.

informed consent of the information subject, the information controller and sharer can also claim the "rational expectation" rule of big data utilization in the specific context to solve the dilemmas of informed consent principle in the age of big data.

2.6.3.3 Crucial public interest rule

If the data processing behavior is to cover a demand of crucial public interest (e.g. COVID-19 prevention and anti-terrorism), in various countries, specific public power departments are given the power to process information without the informed consent of the information subject, in order to deal with the crisis or emergency of public management. However, the above-mentioned information processing behavior must have clear legal provisions and comply with legal procedures, and it must be subject to necessary supervisions and restrictions. The purpose of the processing should be appropriate, and there should be reasonable information protection measures. The concept of crucial public interest should also be explicitly delimited by laws and regulations, so as to avoid the abuse of power by the public power department on the ground of "crucial public interest". To safeguard the crucial public interest is essentially to safeguard the interest of individual, which in line with the general expectations of society and information subject. Crucial public interests can be regarded as a collection of personal interests. Crucial public interest rule is an extreme case of rational expectation rule. However, when it comes to the "general public interest", we should follow the rational expectation rule and carry out risk assessment to determine whether it can be used without informed consent of information subject.

Others, such as the use of personal information on the basis of contract or service improvement in the law of some countries, are actually the extension of the principle of informed consent, which is not regarded as an independent rule in this study. Some countries also stipulate that in emergency situations, in order to better protect the personal interests of the information subject, or to protect the life and health of a third party and other important interests, personal information may be used without informed consent. However, the law cannot define the emergency needs one by one, and the emergency situation cannot be objectively assessed, witch may be a flaw.

Moreover, after the emergency situation is lifted, the information subject should still be informed in an appropriate way.

2.7 Chapter conclusion

The concepts of personal information, personal data, and personal privacy are both related and different. Personal information and personal data are similar concepts, and their denotation and connotation are almost the same. In the common law system, personal information and personal privacy are basically the same, generally more use the expression of personal privacy. In the civil law system, it's generally believed that the category of personal information includes personal privacy, and personal privacy is a subset of personal information. Whether a type of information belongs to personal information can be judged as per the following three features: identifiability, idiosyncrasy, relativity, and the information with anyone of the three features should be judged as personal information. The personal information protection pattern of European and American countries are basically similar to those of Japan and China. The common law countries represented by the United States pay more attention to the use of personal information to promote the rapid development of the data industry, while the civil law countries represented by the European Union pay more attention to the protection of personal information and are cautious about the in-depth development and utilization of data. However, the balance between personal information protection and the development of digital economy should be a trend of data legislation. The protection of personal information in Japan has its own style and relatively perfect development process. It uses the concepts of personal information and personal data at the same time, and strictly protects "special care-required personal information" according to the sensitivity of information. The legislation of personal information protection in China started late, but due to the late-development advantage of laws and regulations, it is supposed that the utilization of personal information in China will be more flexible and the personalized smart services will growth faster. Informed consent is the basic principle of information protection all

over the world. However, in the age of big data, information overload, status asymmetry, data explosion and rapid transmission are challenges to the principle of informed consent.

Chapter 3 Contradiction in Space-time-behavior Analysis Based on Big Data: Anonymization VS De-anonymization

3.1 Introduction

In space-time-behavior analysis based on spatio-temporal big data, mobile phone signaling big data is currently the most frequently used big data sources, which has the remarkable characteristics of dynamic state, high speed, easy access, low cost, and full sample. Mobile phone signal big data not only has space-time dimension, but also has typical human behaviour attribute, which can reflect individual activities in specific temporal and spatial circumstance. Obviously, it belongs to personal information.

In the light of relevant laws and regulations, data related to individuals has been anonymized before being shared and cannot be identified again, that is, if the individual's identity cannot be determined, it will not be considered as personal information.[①] In smart city planning and management, the mobile phone signaling big data is used for building the basic dynamic analysis framework of "space-time-behaviour". Although the mobile phone signal big data is anonymized before being shared, but in some smart city application contexts, it may still show some unique attribute information of the mobile phone user, such as specific location, activity track, etc. We can match the anonymous trajectory data to the associated geographic information space, and mark the location information of the mobile phone user's long-term stay within a specific time period of the day on the map. In this way, it is possible to easily identify specific position information such as mobile phone user's work location and frequent residence. Combining with the activity trajectory information reflects the behavior preferences of rest, entertainment, shopping, sports, etc., it can even give users a detailed portrait. Existing technical means show that in the field of smart city applications, mobile phone signaling big data is easy to de-anonymize, can re-identify mobile phone users, and even accurately portray users.

① *Civil Code of the People's Republic of China (2021)*, Article 1038

Therefore, the anonymization rule does not apply to sharing mobile phone signaling big data for space-time-behavior analysis. Mobile phone signaling big data can reflect people's track information, while the track of activities belongs to sensitive personal information.[①] Once the big data of mobile phone signaling is illegally used or leaked to criminals, it will infringe the information subject privacy, and cause personal and property damage. So, in the space-time-behavior analysis, it is not enough to protect the personal information security if only rely on the existing anonymous measures to share the mobile phone signaling big data.

3.2 Research approach

Firstly, it analyzes the essence of data sharing of mobile phone signaling from the legal level. Then, according to the literature research, it is shown that mobile phone signaling big data is widely used for constructing the basic dynamic analysis framework of "space-time-behavior", and to study the relationship between people life and urban space-time in space-time-behavior analysis in China. In order to protect personal information security, mobile signaling big data is usually anonymized before sharing, that is, the information that can identify users is deleted. However, through patent query, there are many de-anonymization technologies for the mobile phone signaling big data, which have been applied in the practice of space-time-behavior analysis. Next, a simple identification method is proposed, that is, the anonymous trajectory information can be matched to the corresponding geographical space, and then mark the active position information in specific period of time. It can easily identify the specific positions such as work-place and residence of users, and even give users' portraits, which is easy to infringe personal privacy. In smart city planning and management, using mobile phone signaling big data to establish an analysis framework of "space-time-behavior", is actually a process of identifying spatio-temporal data, which can easily lead to the leakage of personal information. Finally, the sharing rules of sensitive personal information such as mobile phone

① *Civil Code of the People's Republic of China (2021)*, Article 1034

signaling big data are discussed to strengthen the effective protection and rational use of personal information in the smart cities planing and management.

3.3 Data sharing: lifeblood of digital economy in the era of big data

Data sharing is one of the main ways to use personal information in the age of big data. The planning based on space-time-behavior often involves data sharing between different information controllers and reusers.

3.3.1 Analysis of the essence of data sharing

Data Sharing is the way that data controller shares the collected information with a third party with or without charge, forming a civil and commercial legal relation on the basis of data right division between the data controller and sharer. The sharer can also be called the data re-using party. In the context of digital economy, big data resource has become an important production factor. And high-level development and usage of data resource is the premise of both information-based improvements in traditional industry and fast development of modern information service industry. Data Sharing is a key way of re-using data resources. By data sharing, it is both available to reduce the cost on data acquisition and make full use of resources.

From the perspective of the information subject, data sharing behavior is essentially the same as personal information recollection.(Wang, 2019) In practical terms, the information sharers are also the personal information collectors, and the sharing behaviors must also be restricted by the principle of informed consent. In general, data sharing should have specific and appropriate purposes. In the case of informed consent of the information subject, personal information can be shared and used legally and rationally. Without the informed consent of the information subject, the personal information shall not be shared and processed exceed the scope of utilization determined just at that moment of it be collected, unless otherwise provided by law or agreed in the contract.[①]

In practice, after sharing personal information, the information subject is possible

① *Civil Code of the People's Republic of China*, Article 1035.

to lose the right of making decision on the personal information. If the personal information is improperly used, the privacy of the information subject may be infringed and the subject may be discriminated against. Furthermore, it is common that the information subject may be defrauded and subject to personal and property damages in case that the personal information is disclosed[①]. If enterprise managers do not process the shared data as provided by law, it is easy to violate the law and even constitute a criminal offence, for instance, crime of infringing citizen's personal information[②].

3.3.2 Sharing of mobile phone signaling big data

As a control command in a mobile telecommunication system, mobile phone signaling is used for its prime technical purpose to control the link of channel and transfer the management information of communication network to uphold the stable operation of the telecommunication system. With the quick advancement of big data technologies, mobile phone signaling big data has the teatures of whole sample, low cost, high volume, high velocity and well time, visually provides the space position, space pattern and time stamp of information. It is used extensively in people-oriented smart city planning, and its technical and economical values have been enormously broadened. That is to say, mobile operators (as data collectors and data controllers) share mobile phone signaling big data, while urban planners (as data sharers) carry out second exploitation and utilization. And it can even be developed and used many times. In view of the fact that mobile phone signaling big data is able to precisely identify users' activity trace, and personal activity track is geared to sensitive information[③], mobile phone signaling big data should be classified as the sensitive personal information according to the relevant laws of personal information protection. Once misused, it is very easy to violate people's privacy and bring about damae to personal and property interests. Therefore, the more strict sharing rules of sensitive information should be applied in sharing and second exploitation of mobile phone

① *Investigation report on the protection of Chinese Netizens' Rights and Interests*（2016）
② *Criminal Law of the People's Republic of China*，Article 253 (I)
③ *Civil Code of the People's Republic of China*, Article 1034.

signaling big data.

About sensitive personal information, from the point of view in protecting personal information safety and trust interests, information control personnel should use clear and popular language to fully, exactly and timely notice information subjects of the purposes, methods and scopes of sharing and using personal information. What's more, the informed consent of the information subject should have a explicit intent or positive behavior, and the keeping silence of the information subject without rejection should not be deemed to consent, except as otherwise expressly specified by law or there is a limpid and definite consensus between the information subject and the information controller before data sharing.

3.4 Anonymization vs de-anonymization: confrontation between the protection and utilization of personal information

The superiorities of using mobile phone signaling big data for people-oriented spatio-temporal planning are very clear. However, mobile phone signaling big data can generate the trajectory of people activities, sharing and using it also make people feel anxious about personal information leakage. *Civil Code of the People's Republic of China* stipulates that:"without consent of a natural person, no personal information shall be illegally provided for any other person, excluding the information through which the specific individual cannot be identified after processing and which cannot be restored". For the sake of safeguard personal information safety, anonymization technologies are widely used for sharing and processing of mobile phone signaling big data.

3.4.1 Anonymization of mobile phone signaling big data

In order to protect personal information security, before sharing and processing mobile phone signaling big data, network communication operator, that is, personal information controller need to use proper information protecting techniques to preprocess the data. Currently, there are two kinds of means in common use to de-identify personal information: One is to modify the original signaling data

according to the need. That is to say, the interference, interchange or difference processing of personal information can cut down the spatio-temporal accuracy of track, so as to accomplish the aim of personal information protection. In whatever way, this type of processing technologies will lead to the distortion of spatio-temporal data, which makes the conclusions less reliable and doesn't meet the needs of space-time-behavior analysis for data accuracy.(Zhou, Li, et al., 2009) The other is to anonymize primordial signaling data by removing its identifier. What is called information anonymization means the process of blocking-up the relevancy between personal information and its subject through the digital model algorithm, so that the identity of personal information subject cannot be identified and the processed information cannot be recovered under current technical provisions. K-anonymity① is a commonly used technology of information protection, which can also be used for anonymity of trajectory information. For any trajectory, there are at least k-1 other trajectories to be converted into the same anonymous ones to construct an anonymity track set, that is to say, there are k indiscriminable track messages in the quasi-identifier, so that the deliberate attackers can not recognize the identity of the special subject of a particular trajectory. K-anonymity controls the maximum risk of data sharing according to the parameter k. Without background knowledge, the deliberate attackers can only identify the true track of a special subject with a probability of 1/k, which protects the security of personal information to a certain extent.

3.4.2 De-anonymization of mobile phone signaling big data

Everything is invariably in the state of mutual promotion and restraint, which is like the relationship between a spear and a shield. So is personal information protection and utilization technologies. With anonymity technology, it is inevitable to produce de-anonymity technology. They contend with each other and advance each other.

3.4.2.1 De-anonymization technology

De-anonymization is a data-mining tactic in essence, which is a technology to re-identify the identity of information subject from anonymous dataset by technical means. For the de-anonymization of matrix dataset, it is generally to match

① https://en.wikipedia.org/wiki/K-anonymity

independent datasets from different sources, identify common attribute identifiers, and set up corresponding links to realize de-anonymization of anonymous information. However, for the de-anonymization of network dataset, it is generally through the implantation or identification of seeds, clarify the relationship between network nodes, and set up node mapping to realize de-anonymization of anonymous information. If someone wants to attack the anonymized dataset and identify the information of a specific individuality, the most frequently used way is to link and match the known datasets from other sources with overlapping identifier attributes. Even if the attacker only has a little information fragment of a certain information subject, and the sensitive attributes of the identifiers are different or dissimilar, he can still mine the relevant information record from multiple information records through chain attack according to his background knowledge, and identify the specific individuality, thereupon then to acquire the privacy information. (Zang and Bolot, 2011)

In pace with the development of artificial intelligence technologies, de-anonymity technique has become advanced to a higher degree. In the near future, *Nature Communications* published a paper by Rocher and Yves-Alexandre de Montjoye (2019) of Imperial College London, introducing a approach of using generative model to appraise whether personal identity could be re-identified from a complete anonymous database. Yves-Alexandre and colleagues developed an AI program that can precisely estimate the probability of re-identifying the identity of personal information subject through anonymous datasets. It is found that only a limited number of attributes are needed to commonly re-identify personal information subject with high reliability, even though the anonymous datasets are imperfect.

3.4.2.2 De-anonymization technology of mobile phone signaling big data in space-time-behavior analysis

In order to further analyze the existing de-anonymization technologies of mobile phone signaling big data, we logged into the official website of the State Intellectual Property Office of China① to retrieve the patent notice. By inputting keywords such as "mobile phone signaling and identification" , we found that as of January 1, 2020, in various application contexts in the field of urban planning, there are twenty-four invention patents associated with re-identification of anonymous mobile phone

① http://epub.sipo.gov.cn

signaling big data. Of which four are authorized and nineteen have passed the effective substantive examinations, and one has been withdrawn for some reason after the announcement. (As shown in Table 3-1)

Table 3-1. Patents of mobile phone signaling de-anonymization technology in China

No.	Application Number	Effective Filing Date	Patent Name	Patent Applicant /Patent Holder	Inventor	Legal Status
1	2015101597226	2015.04.03	Method for recognizing expressway traffic state based on the quality perception of mobile phone signaling data	Jiangsu Transportation Planning and Design Institute Co., LTD. /Jiangsu Xintong Intelligent Transportation Technology Development Co. LTD	Yu Jun, Ji Jinzhang, Zang Zhengbao Shi Zhan, Wang Hui, Xiao Min, Zhu Hongjun.	Authorized
2	2015104524034	2015.07.29	Method for identifying and portraying travel chain of travelers based on mobile phone signaling data	Southwest Jiaotong University	Zhang Jin, Chen Yiheng, Tang Jinsong, Ren Qianyang.	Authorized
3	2015106651759	2015.10.14	Method for road state recognition based on mobile phone signaling	South China University of Technology	Hu Binjie, Zhan Yiwang, Li Xiaohuan.	It's deemed to be withdrawn after the disclosure of the invention patent application
4	201510970023x	2015.12.22	Method for resident rail transit travel mode recognition based on mobile phone signaling data	Chongqing University of Posts and Telecommunicati ons	Luo Jiangtao, Du Yapeng, Cheng Kefei, Tang Gang, Xu Zheng.	Authorized
5	2016106536280	2016.08.10	Method for mobile phone user travel mode recognition based on mobile phone signaling data and navigation route data	Chongqing University of Posts and Telecommunicati ons	Luo Jiangtao, Du Yapeng, Cheng Kefei, Tang Gang, Xu Zheng.	Authorized
6	2017101016886	2017.02.24	Method for user traveling and staying behavior recognition based on mobile phone signaling data	Southeast University	Liu Zhicheng, Yu Jinbin, Wei Yu, Wang Yuran, Lu Jian, Wang Qiao.	Invention disclosure and effective substantive examination
7	2017101901808	2017.03.27	Method for passenger travel route recognition based on track IC card and mobile phone signaling data	Chongqing University of Posts and Telecommunicati ons /China Mobile (Hangzhou) Information Technology Co., Ltd.	Zhao Ruili, Chen Minjun, Wen Liangsheng, Zhang Zhizhong, Chen Yuelong, Cheng Fan.	Invention disclosure and effective substantive examination
8	2017103051831	2017.05.03	Method for population recognition based on mobile phone signaling data	Beijing Transportation Information Center	Wang Jiachuan, Wu Dongdong, Shi Ruixuan, Xiao Randong, Wang Wei, Du Yong, Yu Haitao.	Invention disclosure and effective substantive examination

9	2017109283724	2017.09.22	Mobile high-speed rail user identification terminal based on mobile phone signaling	Jiangsu Zhimou Technology Co., Ltd.	Zhang Zhenwei, Geng Lei.	Invention disclosure and effective substantive examination
10	2017113930854	2017.12.21	Method for bus line recognition based on user mobile phone signaling	Jiangsu Xinwang Video Software Technology Co., Ltd.	Li Yongjun, Wang Xing, Yuan Lufeng, Yan Xuezhi, Cui Jun.	Invention disclosure and effective substantive examination
11	2018100275996	2018.01.11	Method for regional congestion recognition based on user mobile phone signaling data	Jiangsu Xinwang Video Software Technology Co., Ltd.	Li Yongjun, Wang Xing, Yuan Lufeng, Yan Xuezhi, Cui Jun, Zhu Zhiwei, Wang Wenqi.	Invention disclosure and effective substantive examination
12	2018100536407	2018.01.19	Method and system for path recognition based on mobile phone signaling data	Shenzhen University of Technology (under preparation)	Qin, XuTao, Mo ihong, Guo Ying, Zhang Yilin, Li Wei, Zhang Xiongfei.	Invention disclosure and effective substantive examination
13	2018110302330	2018.09.05	Method for airport rail passenger identification based on mobile phone signaling data	Beijing University of Technology	Lu Yao, Chen Yanyan, Lai Jianhui, Zhang Zheng, Mou Zhenhua.	Invention disclosure and effective substantive examination
14	2018110303865	2018.09.05	Method for airport passenger travel OD recognition based on mobile phone signaling data	Beijing University of Technology	Lu Yao, Chen Yanyan, Lai Jianhui, Zhang Zheng, Mou Zhenhua.	Invention disclosure and effective substantive examination
15	2019100777094	2019.01.28	Method for mobile user payment identification based on mobile phone signaling big data	Chongqing University of Posts and Telecommunications	Wang Qianzhu, Yang Xiaoya, Fan Xingrong, Wei Qingxia, Xu Guoliang, Jiang Tao.	Invention disclosure and effective substantive examination
16	2019101928922	2019.03.14	Method and system for population identification based on mobile phone signaling data	Shanghai Tongji Urban Planning and Design Institute Co., Ltd.	Wang De, Yin Zhenxuan, Liu Zhenyu, Zong li.	Invention disclosure and effective substantive examination
17	2019101976184	2019.03.15	Method for identifying source of urban traffic congestion in morning peak hours based on mobile phone signaling	Shanghai Tongji Urban Planning and Design Institute Co., Ltd.	Wang De, Zhang Yuepeng, Zhang Yangfan.	Invention disclosure and effective substantive examination
18	2019102757339	2019.04.08	Method for airport arrival and departure passenger identification and passenger condition analysis based on mobile phone signaling data	Jiangsu Haobai Information Service Co., Ltd.	Liu Linghui, Wang Tuo, Huang Qiangsong, Su Zhengyang, Li Qinglin, Zhang Wen, Sha Wenping.	Invention disclosure and effective substantive examination

19	2019104674222	2019.05.31	Method for identifying population type of railway transportation hub based on mobile phone signaling data	Nanjing Ruiqi Intelligent Transportation Technology Industry Research Institute Co., Ltd	Zhang Gai, Lu Zhenbo, Wan Ziyin, Zhang Jingfen, Zhang Nianqi, Ding Xiangyan, Shi Yufen, Liu Xiaoqing.	Invention disclosure and effective substantive examination
20	2019104671205	2019.05.31	Method for crowd type identification based on mobile phone signaling data	Nanjing Ruiqi Intelligent Transportation Technology Industry Research Institute Co., Ltd.	Zhang Gai, Lu Zhenbo, Wan Ziyin, Zhang Jingfen, Ding Da, Zhang Nianqi, Shi Yufen, Liu Xiaoqing, Ding Xiangyan.	Invention disclosure and effective substantive examination
21	2019105298062	2019.06.19	Method for improved mobile phone signaling data travel identification based on dynamic space threshold	Tongji University	Wang De, Jiang Hetao.	Invention disclosure and effective substantive examination
22	2019105298005	2019.06.19	Method for identifying and correcting spatial deviation of mobile phone signaling data	Tongji University	Wang De, Jiang Hetao.	Invention disclosure and effective substantive examination
23	2019106291465	2019.07.12	Method for user activity space identification based on mobile phone signaling	Chongqing Transportation Planning Research Institute	Zhao Bicheng, Tang Xiaoyong, Gao Zhigang, Zhang Jiansong.	Invention disclosure and effective substantive examination
24	2019106288566	2019.07.12	Method for identifying population migration based on mobile phone signaling	Chongqing Transportation Planning Research Institute	Zhao Bicheng, Tang Xiaoyong, Gao Zhigang, Zhang Jiansong.	Invention disclosure and effective substantive examination

In the above different contexts, states or applications, all the identification technologies of anonymous mobile phone signaling big data can be applied to de-anonymization according to the patent statement in the announcement. As shown in entry 23 of Table 3-1 *Method for User Activity Space Identification Based on Mobile Phone Signaling*. The patented technology proposes a method of space identification about user activity on the basis of mobile phone signaling, which automatically identifies user activity points by building a spatio-temporal clustering model,. This technology can identify the user's activity laws, and then identify the user's living place, work place and the destination of regular activities. It is conducive to accurately and dynamically master the laws and purposes of users' activities, The technology can be applied to space-time-behavior analysis, which contributes to promoting the scientificity of planning and geographical distribution of residential place, production place and various public service facilities in urban, so as to realize people-oriented smart city planning. (Zhao, Tang, et al., 2019)

3.5 A simple identification method is enough to cause privacy risks

In the applied contexts of spatio-temporal big data, the mobile phone signaling is used to excavate the spatio-temporal features of people behaviour track. It's usually matched to geographic information space to build the basic dynamic analysis framework of "space-time-behavior", and study the people-oriented space planning and time planning of smart city, so then to guide healthy and low-carbon behavior pattern. Next, we use the mobile phone signaling big data and a simple space-time-behavior analysis method, specific time-location method, to determine workplace, residence, and other special position information.

3.5.1 Specific time-location method

As far as a specific information subject is concerned, its activity trajectory usually has the features of relatively stability. The anonymous trajectory information can be matched with the relevant digital geospatial through space-time-behavior analysis,

in order to tag the active position of the information subject, which is called specific time-location method. For instance, we can identify the residence and workplace of information subject by tracking some anonymous trajectory information at regular intervals and mining the location information in a specific period of time. It is generally supposed that 9:00 to 12:00 and 14:00 to 17:00 on weekdays are the most likely working time, during which people will be at work. And 24:00 to 6:00 of the next day is assumed to be the most likely home time when people will stay at home. Based on this assumption, for a specific trajectory information, we can observe its position information in the time period of work and home, as well as its continuous stay time and active times. Then the steady location with the most effective times in the working hours could be mainly judged as the working place of the information subject, and the steady location with the most effective times in the home hours can be mainly judged as the residence of the information subject. After that, we can use the relevant datasets obtained from other ways, including the known identity information and the location information of workplace and residence, to match and link the identified sensitive location information according to workplace and residence. This can identify the identity and activity track of information subject with high probability. Go a step further, we can use the side information of a specific information subject's past life got from public network and social media to confirm some key position information at a specific time point, such as travel information, catering information, etc. Then, using space-time-behavior analysis method to compare the track characteristics of anonymous trail information at thr relevant time period, the complete historical activity trail of information subject is identified and obtained.(Zhong, Chang, et al., 2016) Furthermore, we can also determine the frequently visited locations of the information subject reflected by the steady points having more active times in every period of trail information, so as to master the activity law of the information subject.

3.5.2 User portrait and privacy risks

Using the track information reflected by the big data of mobile signaling, we can

not only identify a user's identity, workplace, residence place and activity law, but also carry out user portrait based on space-time-behavior analysis. For example, we can synthesize the mobile signaling big data into an activity trajectory and match it to the geographic information space(as shown in Figure 3-1, it is represented by abstract graphics to protect personal information). Then, we can examine the location information of the steady point where the trajectory is more active. It could be deduced that the user lives in an upscale community by the location information of the time period at home, and it also can be deduced that the user works in a famous university by the location information of the work time period. By analyzing the track of daily activities, we can infer that the user is a female through she often goes to a certain beauty agency on holidays and also can infer that the user has a preschool child by going to a kindergarten at the time of commuting. Through the trajectory, we can even find that the user often goes to a top department store, which can infer the user's consumption preference and so on. According to the analysis of the above trajectory data, we could outline a user portrait of young female intellectuals.

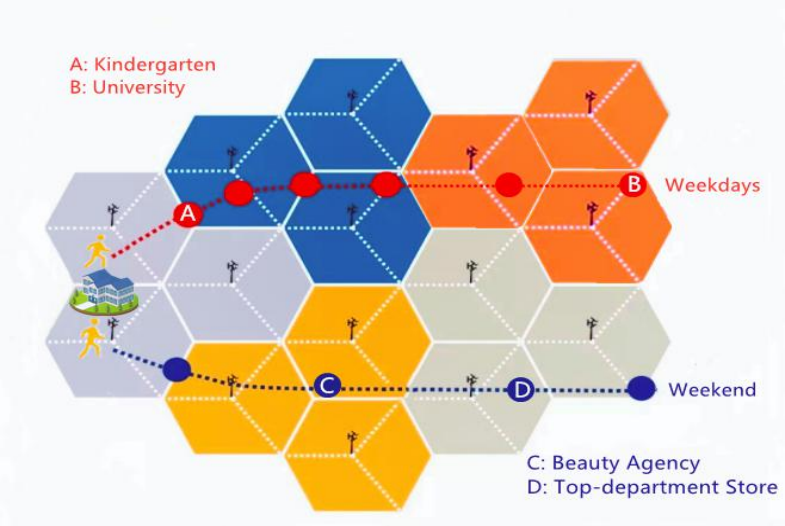


Figure 3-1. User activity trajectory

Obviously, mobile phone signaling big data can form a user's activity trajectory, which is highly identifiable in terms of individual behavior in time and space. Even though it is anonymous, it is easier to be recognized again by using de-anonymization technology. In the age of big data, with the development of mobile signaling big data De-anonymization technology, people's worries about personal information being

inappropriately used or even leaked have been further deepened. Personal activity trajectory belongs to personal sensitive information, and the identification technology of personal activity trajectory is a double-edged sword. The key is to see the technology is used for what, for whom, whether the informed consent of the information subject or legal permission. When it is used in public health emergency management or anti-terrorism, it is very helpful and meaningful. For example, in the fight against covid-19 epidemic, some countries, such as China and Korea, used activity track data of infected people to find close contacts,[①] thus effectively cut off the chain of infection. (Benreguia, Moumen, et al., 2020) When it is used by malicious attackers to infringe the privacy of information subject and even the personal and property safety, the de-anonymization of personal information has huge side effects. Along with the step fore ward of artificial intelligence, cloud computing and other modern information technology, the recognition technologies of track information will only become more and more powerful. Obviously, in the age of big data, it's impossible to anonymize track data completely. However, in the light of the urgent demands for track data in the field of people-oriented urban planning, it's also impractical to completely prevent the sharing and utilization of track information with human behavior such as mobile phone signaling big data. From this point of view, in the present urban planning practice on the basis of space-time-behavior analysis in China, just depending on anonymization rule in sharing and utilization mobile phone signaling big data is far from enough to ensure personal information safety. The key to solving the problem is how to formulate more valid data sharing and using rules to insure that personal information is not illegally used and the security of personal information subject is not infringed.

3.5.3 Rules for sharing mobile phone signaling big data

As mentioned above, mobile phone signaling big data can reflect the track of an individual. In urban planning on the basis of space-time-behavior analysis, there are many existing de-anonymization techniques, so the association between anonymous

①https://blogs.worldbank.org/eastasiapacific/koreas-response-covid-19-early-lessons-tackling-pandemic

data and information subject cannot be completely blocked. For this reason, in the people-oriented urban planning, it is far from enough to share the mobile phone signaling only by anonymization rules rule. Therefore, in the age of big data, through the research on the current urban planning practice in China, we found that it is not appropriate to use a lot of "anonymous" mobile phone signaling big data without the consent of the information subject. Obviously, there is a great legal risk of violating personal information safety.

The rule of rational expectation is a possible alternative. It is closely relevant to the general cognition and expectation of the society to protect personal privacy, and should meet the reasonable expectation of most information subjects for the personal information protection. In terms of the sharing and use of personal information, Chinese hold a more tolerant attitude about mobile phone signaling big data sharing. Although they also care for personal information protection, they are more willing to exchange part of their privacy for convenient services, so that personal information can be used reasonably. But in Europe, American and Japan, affected by different values, people have different cognition and expectations of privacy protection. In some cases, they would rather sacrifice convenience than compromise easily. (ZENG, 2007) Consequently, it's necessary to identify the sensitivity of personal information and accurately define the "rational expectation" of the information subject. If the sharing data belongs to sensitive personal information such as mobile signaling, the "rational expectation" of the information subject is also limited. (Wang, 2019) It needs to be clearly stipulated in the law, also needs an independent and objective risk assessment of sharing mobile phone signaling for specific application scenarios.

In a sense, people-oriented urban planning with spatio-temporal big data, especially in terms of urban public management, is also a need of public interest. Nevertheless, the definition of public interest is not consistent in different countries all over the world.. Generally speaking, urban planning and management do not belong to the crucial public interest. Unless it is related to urban public security or emergency, and it must be plainly defined by legislation and has undergone legal proceedings, the sharing and processing of mobile phone signaling big data in urban

planning must still follow the principle of informed consent or within the rational expectation of the information subject. In many countries, including China and Korea, if personal trajectory information is used to meet the needs of emergency, it can be used urgently according to the crucial public interest rule. For example, in a public health emergency state, the mobile phone signalling big data can be use to track the activity trajectory of COVID-19 infector, and find their close contacts. The purpose is to prevent and control the epidemic and protect the life and health of the public. At this time, the use of personal trajectory information will not be adopted the principle of informed consent. Of course, in order to track close contacts, another technical route that European and American countries prefer to try is to develop digitized contact tracking by the aid of mobile phone App and Blue Tooth, but the premise is that mobile phone users voluntarily install tracking software. (Dai, 2020)

To sum up, the spatio-temporal big data, such as mobile phone signaling big data, which can form a person's track, belongs to sensitive personal information. Once it is abused or leaked, it's very likely to violate the information subject privacy and damage his personal and property rights. In general, when sharing and using spatio-temporal big data, it is necessary to fully, exactly and timely notify the information subject the purpose, mode and range of utilization in easy to understand terms. That is to say, the consent and explicit authorization of the information subject should be got beforehand, and the independent expression of wish should be ensured on fully knowing the situation. However, in the age of big data, the principle of informed consent can not fully adapt to the massive, dynamic and fast transmission of spatio-temporal big data such as mobile phone signaling big data. We can consider using the rule of rational expectation, and even use the rule of crucial public interest in the case of public safety, as a supplementary choice of the principle of informed consent.

3.6 Chapter conclusion

The sharing and utilization of spatio-temporal big data not only provides new

thinking, new technique and new solution for people-oriented urban planning, but also brings a new controversy about personal information protection and rational utilizstion. Data sharing is essentially a data collection and reuse so the informed consent principle is also the fundamental principle of data sharing. In people-oriented urban planning based on space-time-behavior analysis, anonymous mobile signaling big data can be de-anonymized and identify personal activity trace. So, anonymization rule is not suitable for the sharing of mobile phone signaling big data in space-time-behaviour analysis. From the practice of China's urban planning, we can see that only depending on "anonymization" method to share and use mobile phone signaling big data, there are serious risks of infringing personal privacy and even causing the loss of personal property of the information subject. According to the current laws, in the space-time-behavior analysis, the sharing and use of sensitive personal information such as mobile phone signaling big data should get the informed consent of the information subject. In the age of big data, the principle of informed consent is facing difficulties in application relevant to spatio-temporal big data, and the rule of rational expectation can be used as a possible supplementary option.

Chapter 4 Personal Information Protection and Interest Balance Based on Rational Expectation

4.1 Introduction

In the era of big data, massive diverse dynamic data is generated in the context of massive "digitalization". Big data greatly facilitates people's daily life. For example, decision on selection of daily travelling route and even planning for personal career can all be made with the assistance of big data. Meanwhile in the field of market management, big data is used for providing personalized services, which enormously improves the operators' profitability while bringing people convenient life and improved quality. Government sectors also make use of big data to promote e-government, intelligent management, and social governance, make scientific and rational decisions, and better provide public services. However, personal information has also been shared at will, used in violation of regulations, or even disclosed in large amount so that the personal privacy and personal property safety of the information subject are facing threats.

With the improvement in computing power and the emergence of Internet of Things and 5G communication technologies, the processing efficiency and transmission rate of personal information have increased greatly, making data sharing increasingly easy. Driven by interests, a large amount of personal information is shared. Consequently, relevant stakeholders are becoming diverse, and the interest demands of different stakeholders overlap and even conflict with each other. Facing the challenges of personal information protection and utilization in the age of big data, the traditional principle of informed consent becomes less operable and costs high. (Tian, 2018)

In 1999, Spiros Simitis first proposed Context-oriented Rules in the investigation report on the implementation of *Convention for the protection of individuals with region to automatic processing of personal data*. And insisted that there is a need to consider the sensitivity of personal information based on the specific context, and take

corresponding protection measures accordingly.[①] Nissenbaum (2004) further put forward the theory of "Contextual Integrity", which holds that the specific context of the original collection of personal information should be respected, and its subsequent dissemination and use should not exceed the situation at that time. That is, in a specific context, the information processing should consistent with the expectations of the information subject, and the specific information processing should match the specific context. Personal information collected in a specific context shall not be processed beyond that context. She believes that the key to protecting personal information is to ensure the "Contextual Integrity" of the flow and utilization of personal information.

The context is composed of many factors, and the influence of different factors is different, and that the risk may be different after the combination. How to judge whether the personal information processing context exceeds the rational expectation of the information subject, we need to introduce the risk management methods to evaluate the risk degree of the application context, so as to ensure the safety of personal information processing behavior. Through risk assessment, the risk of personal information processing can be controlled within the rational expectation of the information subject. Information processor should also carry out risk management in all aspects of personal information processing.

In this chapter, from the perspective of balancing the interests of personal information subjects, business entities and public managers, it discusses the mode of protection and rational utilization of personal information based on rational expectation rule. Further, the criteria for judging rational expectations are proposed by assessing the risk of personal information in specific application contexts, to realize the effective protection and rational utilization of personal information.

4.2 Research approach

Firstly, through the analysis of the value of personal information and the

① Review of the answers to the Questionnaire of the Consultative Committee of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS 108), 1999.

measurement of interests, this chapter defines the core interests of personal information subjects and the relationships among the protection of personal information, the development of digital economy and the maintenance of public interests. For the purpose of protecting personal core interests and balancing the interests among stakeholders, the risk assessment model is constructed：

R (I, T, V) =R (P(T, V), S (T, I))

Then, the criteria for determining rational expectations were discussed through the risk assessment on personal information by using matrix method in specific context. And rational expectation rule is proposed to balance the interests of personal information subjects, business entities and public managers, so as to protect and rationally use personal information in the era of big data. Finally, taking the application of mobile phone signaling big data in space-time-behavior analysis as an example, through using rational expectation rule, the combination of quantitative analysis and qualitative analysis to simulate the application of personal information sharing in the specific context of smart city planning and management.

4.3 Diversified stakeholders of personal information in the era of big data and their interest demands

In the age of big data, people's life is being changed profoundly by information technology (IT), computing power and artificial intelligence (AI). The innovative application of big data even stimulates huge economic and social values but also brings legal problems about rational use of personal information.(Zhou, 2019) In the process of data sharing, diversified stakeholders are involved and the interest conflict between personal information subjects, business entities and public managers is becoming prominent. It is urgently needed to balance the stakeholders' interests for the sake of ensure rational use and protection of personal information. Value determination is an important factor of risk assessment, and the premise of the application of rational expectation rule and the realization of benefit balance.

4.3.1 Analysis of the values of personal information

4.3.1.1 Personality dignity and freedom value of personal information

Sensitive information in personal information often involves personal privacy and thus is protected by personality right. While personality right taking personality dignity and freedom as the value basis is the specific embodiment of personal dignity value and makes it possible to realize independence and free development of personality (James, 2004). The term of "personal dignity" was mentioned in the *Charter of the United Nations* (1945) for the first time and initially confirmed as a basic human right in form of legal document in the *Universal Declaration of Human Rights* (1948). Personality dignity itself has specificity and thus that of personal information subject is maintained by law,[①] which prevents others from infringing sensitive personal information and provides precondition for personal information subject to exercise his/her personality right. A person's personality dignity is equally protected by law regardless of his/her family background, wealth and status, which precisely reflects the core value of personality dignity. With the development of society, various new personality interests appear especially in the age of big data. Whether to incorporate the interests in the protection range of personality right or not should be determined on the basis of personality dignity.[②] So, personality dignity and freedom is the core value of personal information.

4.3.1.2 Economic use value of personal information

The economic use value of personal information is closely relevant to the substantial improvements in data acquisition capacity, storage capability and computing power based on big data and the resulting changes in industrial production mode and commercial marketing model. With the development of IT and AI technologies, data resource has become one of the five core production factors,[③] and the deep integration of informatization into economic and social development has greatly affected industrial division and the adjustment of business conditions and

① *Civil Code of the People's Republic of China (2021),* Article 109
② *Civil Code of the People's Republic of China (2021),* Article 990
③ *Opinions of the State Council on Improving the Systems and Mechanisms for Market-based Allocation of Factors of Production（China, 2020）*

reshaped the competition pattern of world economy. Supported by big data technology, production can be carried forward under the condition of accurate understanding of consumer demand. Commercial marketing has also been transformed from the early massive advertising to oriented marketing and data pushing in due time, resulting in significant increase in economic efficiency. And the integration, sharing and use of information have become a new profit source for enterprises. Meanwhile, operators have elaborately improved their products and services taking consumer demand as the orientation, which greatly meets consumer demand and improves consumer experience. Overall improvement in the use level and economic value of personal information resources is the objective needs of economic development in the age of big data.

4.3.1.3 Public management value of personal information

Personal information contains public management value. Since ancient times, rulers of various countries in the world have always been collecting and using personal information to govern the country. The census conducted by government body is a traditional way of collecting and using personal information. In 4500 BC, the ancient Kingdom of Babylon had conducted national census; and the world first modern census was conducted in America in 1790. By virtue of advanced information technology in the age of big data, governments of various countries can collect and use personal information more quickly at low cost, determine social conditions and public opinions by making extensive specimen analysis, make scientific and rational decision and better boost public management and public service. Personal information of criminal suspect can be used by relevant government sector to effectively trace the clues and make information analysis, so as to hit and prevent crime and fully guarantee public safety. Meanwhile, personal information of epidemic patient can be applied in public health field to timely trace and cut off the transmission route of the epidemic, effectively preventing the transmission of epidemic such as COVID-19. (Benreguia , Moumen, et al., 2020)

4.3.2 Diversified stakeholders of personal information and their interlaced interest demands

Due to the multiple values of personal information, diversified stakeholders have different and even conflicting interest demands for personal information. According to the analysis on the values of personal information, the stakeholders of personal information can be divided into three categories: personal information subjects, business entities and public managers. Among them, business entities can be further divided into the traditional industrial operator transforming to information-based operation model and the service provider engaging in supply of data resources. While public managers also include the central government, local government and third-party institutions, such as industry associations authorized by government.

4.3.2.1 Interest demands of personal information subject

First, personal information subject not only treat personal information as a kind of "data resource" but also has the demand for protecting the sensitive information involving personal privacy and the personality interest contained in his/her personal information by law. In the context of big data, the terminals of Internet of Things can collect personal information in almost the entire time and space. Consequently, the virtual nature and anonymity of cyberspace and the convenience in information transmission stimulate more intensified demand for protecting personal privacy. And this demand has evolved into general demand of the whole society.(Wang, 2021a) Second, with the economic use value and public management value as discovered by big data mining technology, non-sensitive information in personal information has become a "data asset" that can bring huge interest and the personal information subject has the right to enjoy the interest and process it.[①] Third, in the age of big data, the whole society has intensified dependence on information resource. Even the persons involved in the informatization progress may use relevant information service provided by public and private institutions to meet their daily living needs. Hence, individual is required to alien certain personal information to meet the entire society's demands for information product and service supply.

① *General Data Protection Regulation* (EU, 2018)

4.3.2.2 Interest demands of business entities

With the development of digital economy, business entities have increasingly high demand for using personal information. Traditional business operators can collect and process customers' personal information to know about the market demand to make targeted production and sales plan and thus improve the profitability. Due to the extensive demands for personal information, personal information service providers specialized in collection, storage, transmission and supply of information have also emerged. By collecting large amount of personal information and analyzing and digging the information by certain rules, they have constructed various databases to provide information service with or without charge and meet the special and individualized demand of economic production for data resources. Meanwhile, large e-commerce transaction platform and social networking services collect massive personal information from the extensive transaction data and social data by virtue of their channel advantages so that they can provide extended information service and serve as specialized information providers to obtain excess earnings beyond the main business, while improving their service quality and economic efficiency.

4.3.2.3 Interest demands of public managers

It has become a common practice in countries all over the world to collect and use necessary personal information under legal framework to better provide public service and administrate the society.(Zhang, 2021) As government management and service is oriented to people, various personal information is surely necessary to be obtained and positively used in order to guarantee public safety, provide public service an realize effective social governance, which is also the intrinsic demand of "people-oriented government". The public managers represented by the government are always the greatest collectors and users of personal information and also the protectors of such information.(Zhang, 2015) As the authority of public power, government is responsible for protecting citizens' personality rights and property rights and interests and cannot collect and use personal information at will, and its way and extent of using personal information should be restricted by law. Public power cannot be exercised without written regulations in law. Collection and disposal of personal information by government is restricted legally, which is not only a reflection of respecting human rights but also is needed for protecting equal competition in the market and more for maintaining social stability and the validity of the government's political power. The government should formulate basic policies for

the protection of personal information for the sake of seeking comprehensive and complete measures to promote the protection of personal information. The central government should formulate guidelines to ensure that business entities act appropriately and effectively, and take other integral actions to support the personal information protection measures formulated or implemented by local governments, domestic residents or business entities to seek proper processing of personal information.[①] The local governments, for the sake of ensuring the proper processing of personal information, should try to take necessary actions to support the business entities and residents in local region.[②] The Local government can use large amount of personal information to improve public management and service quality, and also promote economic development by regulating business entity's rational use of personal information while fully protecting sensitive personal information to maintain social stability. The government can also authorize professional third-party organizations, such as industry associations, to formulate the implementation norms of personal information protection and reasonable utilization in relevant fields, so as to make the protection and utilization of personal information more practical.

In summary, personal information bears personal interests, economic interests and public interests. Respecting and protecting personality dignity is the core interest demand of personal information subject, and also the premise of the protection and rational utilization of personal information.

4.4 Rational expectation based on risk assessment of personal information in specific application context

4.4.1 Rational expectations: new option of personal information protection model in the era of big data

The principle of informed consent is the basic principle for personal information protection[③]. In the age of big data, with the breakthrough in computing power, and the emergence of IoT and 5G communication technologies, the processing efficiency and transmission rate of personal information have been greatly improved. Followed by,

① *Amended Act on the Protection of Personal Information* (Japan, 2016), Article 8
② *Amended Act on the Protection of Personal Information* (Japan, 2016), Article 12
③ *The Privacy Act* (USA,1974)；*General Data Protection Regulation* (EU,2018)；*Civil Code of the People's Republic of China* (2021).

data is shared for many times and used for uncertain purposes. This case increases the difficulty in applying the principle of informed consent so that the traditional protection model oriented to informed consent is confronting with great challenge.(Fan, 2016) To evade legal risk and meet legal requirement for informed consent, business entities often list tedious and obscure privacy policies that are difficult to be read and understood by users.(McDonald and Cranor, 2008) In order to use the product or service, user has to passively accept the privacy policies so that the policies become non-sense and cannot provide personal information subject substantial guarantee.(Choi, Park, et al. 2018) In need of using massive dynamic data, for instance using mobile phone signaling big data to make planning for smart city(Manfredini, Pucci, et al. 2014), it is less feasible to obtain informed consent of the information subject in practice. Hence, only on the principle of informed consent, it has already been difficult to adapt to the current economic and social development trends and not available to effectively balance the interests among personal information subjects, business entities and public managers. In the age of big data, the rule of rational expectation has become an innovative option of personal information protection[①]. Whether a personal information processing behavior gets in breach of the right and interest of information subject can be judged by measuring the information subject's rational expectation for protection and utilization of personal information in specific application contexts (Nissenbaum, 2009). In other words, in specific context, a behavior of collection and sharing of personal information is rational even without informed consent of the information subject, provided that the behavior is expectable for relevant parties and can be generally accepted by the society and the risk of sharing or collecting information is under control. From the perspective of interest balance, the target of personal information protection is to make rational use of personal information on the premise of strictly protecting personality dignity of the information subject. Definition of the circumstances of rational use constitutes the "boundary" of personal information protection. What rational expectation is on earth and whether the expectation complies with common social cognition or not should be

① *General Data Protection Regulation (EU,2018)*；*Consumer Privacy Bill of Rights Act (Draft)* (USA, 2015)

judged by making risk assessment on the shared personal information in specific context, namely admitting the necessary existence of risk and getting the risk controlled within acceptable range.

4.4.2 Risk assessment on personal information in special context

Risk assessment on personal information is a process to test the legality and compliance of personal information processing behavior, judge the risk level of this behavior to damage legal right and interest of personal information subject, and assess the effectiveness of various measures taken for protecting the subject[①]. This risk assessment should obey the laws or the industrial standard formulated with legal authorization, integrate many subjective and objective factors, make specific survey on the protection and utilization of personal information in specific application contexts and analyze and judge the possibility of the behavior to cause risk and the severity of the harm caused by the risk. European Data Protection Board suggests that Data Protection Impact Assessment (DPIA) should be carried out before processing any data involving innovative technologies (e.g. AI and machine learning) and sensitive personal information (e.g. biological data, health data and credit data) and tracing the location or behavior of person[②].

4.4.2.1 General flow of risk assessment on the sharing of personal information

At present, European and American countries have established their specific information risk assessment standards which provide risk prevention and control tools for protecting personal information[③]. In specific context, general flow of the risk assessment is as shown in Fig. 4-1:

The first is to comprehensively sort out the personal information to be assessed and form a complete list of shared data and data flow charts, and focus on describing the type, amount, sensitivity, anonymization, and cross-border transfer of personal information.

---

① *Information security technology—Guidance for personal information security impact assessment* (China, GB/T 39335-2020)

② *Guidelines on Data Protection Impact Assessment (DPIA)* (European Data Protection Board, 2017)

③ *Information technology-Security techniques-Privacy impact assessment* (ISO/IEC FDIS, 2017); *Handbook on Security of Personal Data Processing* (ENISA,2017); *Guidelines on Data Protection Impact Assessment* (ICO, 2017)

The second is to confirm with the data sharer the application contexts of the personal information to be assessed and focus on describing the identity of third party of the sharing, the purpose of processing personal information, detailed processing method, safety measures to be taken in the processing process, the persons having access to personal information, the status of third party's access to information systems, the list of interfaces for external transmission of personal information, data storage and deletion plans, and the disposal of storage media, and so on.

The third is to identify possible threats (including threat sources, affected objects, occurrence probability and frequency) in personal information processing in this context, generally from the aspects of network environment and technical measures, personal information processing flow, third parties and participants, business characteristics, scale, and security situation.[①].

The fourth is to analyze possible threats and assess the existing vulnerabilities in this context, judge the efficiency of current security measure for guaranteeing data sharing (security management guarantees and security technical safeguards for special data recipient) and assess whether the rights and interests of personal information subject are possible to be harmed or not.

The fifth is to assess the values of personal information and the interests of personal information subject, and analyze the possible impact of the threats identified in this context on the rights and interests of personal information subject and the impact extent. This impact can generally be measured from the following dimensions: the restriction in information subject's right to make decisions independently, infringe personality dignity (e.g. the possibilities to trigger discriminatory treatment), and harm personal and property safety.

The sixth is to generate a two-dimensional risk judgment matrix based on two results to judge the risk level of the personal information processing and judge whether the big data is used within safe range of rational expectation or not.

The seventh is to put forward applicable improvement suggestions to complete

① *Information security technology—Guidance for personal information security impact assessment* (GB/T 39335-2020)

the security guarantee measures and finally form the assessment conclusion.

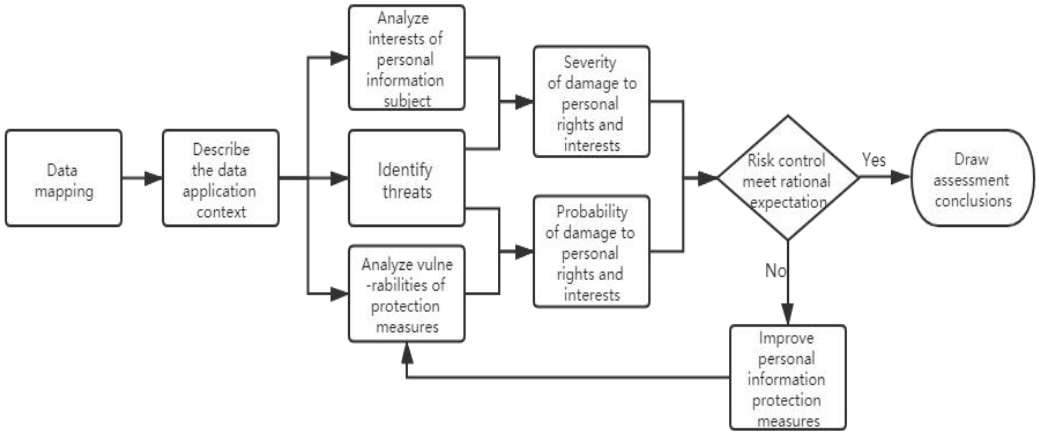


Figure 4-1 General flow of risk assessment on the sharing of personal information

4.4.2.2 Calculation model of the risk of personal information sharing

To calculate the risk, it is necessary to determine which factors affect the risk, the interaction between the factors and the specific calculation method. In the risk assessment of personal information sharing, the impact factors involved in the calculation of risk value are generally information subject interest, threat and vulnerability, and the interaction between the factors is shown in Figure 4-1. Firstly, the interest, threat and vulnerability of personal information are identified (according to the existing security measures). Then, through the impact of possible threats and the vulnerability of existing security measures, the possibility of harm to the right and interest of personal information subject is determined. And through the impact of threats and the importance of information subject interests to determine the extent of damage to the rights and interests of personal information subject. The damage to the right and interest of the personal information subject generally includes the restriction of the information subject's independent decision-making power, the violation of humanity dignity (such as causing discriminatory treatment), and the injury of personal property. The judgment of the degree of damage should also refer to the result of the possibility of damage, and the loss can not be calculated if the probability of damage is very small (such as the earthquake threat in the non seismic zone).

The basic model of risk calculation is as follows:

R (I, T, V) =R (P(T, V), S (T, I))

Among them,

R - Risk of damage to the rights and interests of personal information subject in a specific context

P - Possibility of damage to the rights and interests of personal information subject caused by threat exploiting vulnerability

S - Severity of damage to the rights and interests of personal information subject caused by the threat

I - Interest of personal information subject

T - Threat considering the probability of threat occurrence and its harmfulness

V - Vulnerability according to existing security measures

The values of the three factors I, T, and V can be determined through statistical analysis or professional experience.

The calculation of the three functions of R, P, S can adopt qualitative analysis method or quantitative analysis method, or combine qualitative and quantitative.

Qualitative analysis is a widely used method, which needs to be graded for each factor of risk by virtue of the knowledge, experience and intuition of the evaluator, or the standards and practices of the industry. Qualitative analysis is relatively easy to operate, but it may also lead to inaccurate analysis results due to the bias of evaluator's experience and intuition, especially the determination of personal information value is greatly influenced by cultural factors. Quantitative analysis gives numerical values to each factor of risk. The mathematical model of comprehensive evaluation is established by measuring the interactions among factors of risk, so as to complete the quantitative calculation of risk. Quantitative analysis method is more accurate, but because of many application contexts of personal information, the types of personal information used are different, the judgment of the interest of personal information subject is affected by many factors, and the threats and vulnerabilities are also different, so it is relatively difficult to build a system risk model. The combination of qualitative and quantitative analysis method is to assign and calculate the risk factors, and adopt qualitative and quantitative methods according to the need. It can be adjusted appropriately and necessary for different context, and has great

flexibility. The matrix method is a qualitative and quantitative method that is commonly used in the current risk calculation.

4.4.2.3 Matrix method to calculate risk of personal information sharing

The Matrix Method is mainly applicable to the case that the target element value is determined by two known element values. Firstly, a two-dimensional calculation matrix is constructed. The value of each element in the matrix can be determined according to the specific situation, and it does not necessarily follow a unified calculation formula, but it must have a unified increasing and decreasing trend. Then, the values of the two elements determined are substituted into the matrix for comparison, and the intersection of rows and columns is the target element The calculation result of prime value. Namely:

$z=f(x, y)$

$x=\{x_1, x_2, \ldots x_i, \ldots x_m\}, 1\leq i \leq m, \quad x_i \in N$

$y=\{y_1, y_2, \ldots y_j, \ldots y_n\}, 1\leq j \leq n, \quad y_j \in N$

A two-dimensional matrix is constructed based on the values of element x and element y, as shown in Table 4-1. The matrix row values are all values of element x, and the matrix column values are all values of element y, and m×n values in the matrix are the values of element z. $z=\{z_{11}, z_{12}, \ldots z_{ij}, \ldots z_{mn}\}$, $1 \leq i \leq m, 1\leq j \leq n, z_{ij} \in N$.

Table 4-1 Construction of Matrix

	y	y_1	y_2	⋯	y_j	⋯	y_n
x	x_1	z_{11}	z_{12}	⋯	z_{1j}	⋯	z_{1n}
	x_2	z_{21}	z_{22}	⋯	z_{2j}	⋯	z_{2n}
	⋯	⋯	⋯	⋯	⋯	⋯	⋯
	x_i	z_{i1}	z_{i2}	⋯	z_{ij}	⋯	z_{in}
	⋯	⋯	⋯	⋯	⋯	⋯	⋯
	x_m	z_{m1}	z_{m2}	⋯	z_{mj}	⋯	z_{mn}

For the calculation of the z_{ij}, according to the actual situation, the following formula can be used:

$z_{ij}=x_i+y_j$ or

$z_{ij}=x_i \times y_j$ or

$z_{ij}=\alpha x_i+\beta y_j$, among which, α & β are positive constant.

The calculation of z_{ij} values in the matrix does not necessarily follow a unified formula, but it must have a unified trend of increase or decrease, that is, if f (x, y) is an increasing function, the value of z_{ij} should increase with the value of x_i and y_j, and vice versa.

The characteristic of Matrix Method is that it can clearly list the change trend of elements by constructing the calculation matrix of pairwise elements. It has good flexibility and is widely used in risk analysis.

4.4.2.4 Risk levels of sharing personal information

By identifying the risk source of data sharing in specific context and taking current personal information guarantee measures, the possibility of the sharing to harm the information subject's rights and interests was assessed and generally divided into three levels: considerably possible, rationally possible, and less possible. By analyzing the types of harm that data sharing in the specific context might cause to the information subject's rights and interests according to the possible impact of the identified risk on the information subject's rights and interests, the harm degree was comprehensively assessed and generally divided into three degrees: severe harm, moderate harm, and small impact. Further, by analyzing the possibility to harm the personal information subject's rights and interests and the harm degree, a two-dimensional matrix was constructed as shown in Fig.4-2 to judge the risk level of sharing data in this context.

Risk level		Possibility of damage		
		Less possible	Rationally possible	Considerably possible
Severity of damage	Severe harm	Low risk	High risk	High risk
	Moderate harm	Low risk	Medium risk	High risk
	Minimal impact	Low risk	Low risk	Low risk

Figure 4-2 Matrix for Accessing the Risk Level of Sharing Personal Information

4.4.3 Judgment of rational expectation

If the sharing risk assessed as per Fig.2 is at the level of low risk, the sharing and utilization of personal information in this context complies with the rational expectation. If the risk assessed is at the level of medium risk, it is necessary to take steps timely and actively to reduce the risk and reassess the risk. If the risk assessed is at the level of high risk, the rule of rational expectation doesn't apply and the personal information controller must significantly inform the information subject before sharing the personal information. In this case, data sharing can be carried out only after obtaining user's consent. If there are multiple risk points in the application context, when and only when each risk level judged must be low risk, the rational expectation rule can be applied. It must be noted that the risk assessment and judgement of rational expectation must be made by an independent third-party assessment agency or industry association authorized by law.

4.5 Interests balance of diversified stakeholders based on rational expectation

In the age of big data, personal information not only has the attribute of personality interest, but also has the attribute of economic interest and public interest,

becoming a data asset that can significantly create economic value and social value. For the sake of protecting the core interest of personality dignity and freedom, the personal information subject will benefit from the rational utilization of personal information, such as obtaining the economic interest and/or convenient service. From the view of economic interest, business entities make the best of personal information to maximize the economic interest from business activities and become an independent stakeholder. To better provide public management and public service, governments substantially take part in collection and utilization of personal information, leading to increasingly weakened private right and gradually enhanced public interest of personal information. At present, big data including personal information has become an important national strategic resource, and the protection of personal information security is also the need of national security.

In the face of new technologies such as ICT, IoT and AI, natural person as the subject of information is becoming more and more "transparent" and has intensified intrinsic demand for protecting personal information, but is unable to prevent personal information from being used by others at will. How to balance the interest demands among personal information subjects, business entities and public managers has become an urgent practical problem to be solved. Among the said types of interests, the most important and fundamental interest is personality dignity interest. Strictly protecting personality dignity is a common value[①]. And only in this way can it be possible to balance the interests of the stakeholders and make rational use of personal information. Otherwise, other interests will be like water without source. Provided that the core interest of personal information subject is fully guaranteed, it is crucial to construct rules for balancing the interests of stakeholders based on rational expectations so as to protect and make rational use of personal information (Figure 4-3).

① *Universal Declaration of Human Rights* (UN,1948)

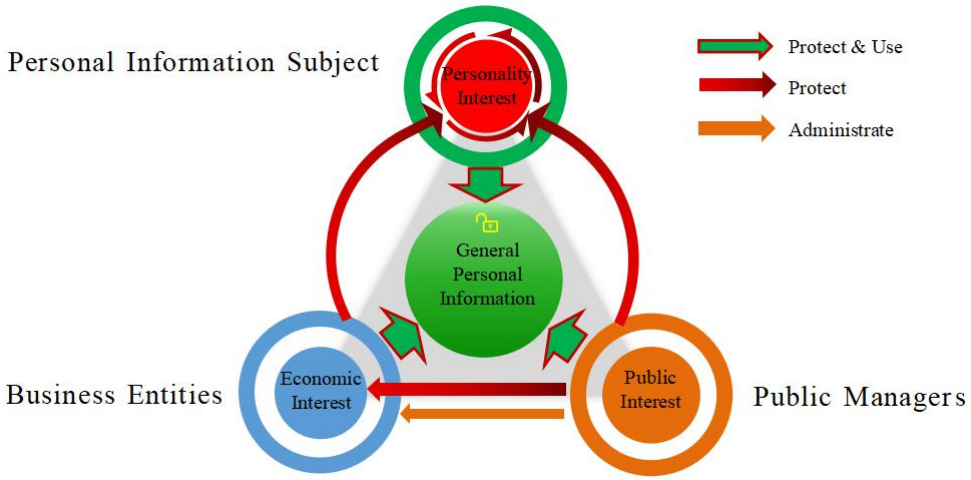


Figure 4-3 Interest Balance between Personal Information Subjects, Business Entities and Public Managers

For public managers, complete personal information protection laws and regulations or industrial standards should be formulated to strictly protect sensitive information involving personality dignity in personal information. Operable laws and regulations and industrial standards should be formulated to ensure that business entities use big data legally and rationally, specify business entities' behaviors of collecting, using and sharing personal information, restrict personal information from being used for unfair competition in breach of rules, and strictly hit the criminal behavior that seriously infringes personal information.[①] In need of collecting, processing and sharing personal information for the purpose of public management and service, the related laws for public use should be formulated in advance and authorized legally, but the capacity of exercising public power should be self-restraint and not over intervene in private rights and interests. To improve the efficiency of public management and public service level, government sectors should authorize partial function of public management to specialized third-party agency such as industrial association to participate in and even lead the collection, utilization and sharing of personal information in relevant field.[②]

For business entities, it is extremely important to obey the laws and regulations and industrial standards for personal information protection, not abuse big data

① *Amendment (IX) to the Criminal Law of the People's Republic of China* (2015)
② *Consumer Privacy Bill of Rights Act*（*Draft*）（USA, 2015）

resources to monopolize or use asymmetric information to make discriminatory transaction, so as to maintain a good business environment. Business entities should respect the private right and interest of information subject and improve the level of guaranteeing personal information safety from the perspectives of operation concept, safety regulations and technological means. Personal information should be obtained or shared legally and used rationally and appropriately[①]. Business entities that control personal information should guarantee the personal information subjects have necessary rights to control the personal information, such as the right to know, the right to correct, the right of being forgotten, restricted processing right, the right to carry and the right to reject[②]. Business entities should comply with general social expectation for protecting and using personal information and give the information subject rational price (economic compensation or convenient service). Business entities should not blindly pursue maximum use of personal information. Only if personal information is protected legally can it be possible to get consumers' trust, maintain fair competition between information service providers and maintain the interests of the business entity itself.

Personal information subject should maintain "rational expectation" for the utilization of personal information in the age of big data, understand that only if being used collectively can personal information give play to its economic value and social value to the maximum extent. For non-sensitive information not involving personal privacy, the information subject can alien it to business operator for rational sharing and use, provided that there are credible laws and technologies to guarantee the security, in order to obtain convenient life and corresponding economic price. Based on public interest and on the premise of getting legal endorsement, public sectors are allowed to collect personal information to obtain better public service and public security guarantee. Sensitive information involving personal privacy is relevant to freedom and dignity of the information subject and thus should be strictly protected by law and should not be processed at will even getting consent of the right holder.

① *Civil Code of the People's Republic of China* (2021), Article 111, Article 1035.
② *General Data Protection Regulation* (EU,2018)

(Wang, 2021b) It is neither allowed to infringe the personality dignity of the information subject for any reason or in any way nor allowed to break the baseline of law and ethic.

4.6 Case study: risk assessment and context simulation

We simulate the case of mobile phone signaling big data sharing in specific context of smart city planning, and explore the application of rational expectation rule based on risk assessment in specific context.

4.6.1 Description of the context

Mobile phone signaling big data is often used for space-time-behavior analysis. As a control signal in the mobile telecommunication system, mobile phone signaling is initially used to control channel link and ensure the stable operations of system. It has the features of full sample, low cost, dynamic and continuity, which directly provides people with the space position, time distribution and behavior identification. Now it is widely used in the field of urban planning based on space-time-behavior analysis, and its technical and economical values have been greatly expanded. Therefore, taking mobile phone signaling big data as an example, the following simulates and discusses the application of rational expectation rule in space-time-behavior analysis.

Application context 1: Measure the hierarchical structure of urban system

Big Data: Mobile phone signaling big data

Data size: Exceed 100 million

Number of information subjects involved: 1.3895 million

Sharing mode: Operation in the physically isolated data system of Telecom Operator

Grid cell size: Take town as a cell

Study area: Chang-jiu urban agglomeration, China

Sources: China Unicom

Application context 2: Study the spatial characteristics of urban activities and community differentiation

Big Data: Mobile phone signaling big data

Data size: Exceed 100 million

Number of information subjects involved: 1.6463 million

Sharing mode: Transmission to the data system controlled by researcher

Grid cell size: 200m×200m

Study area: Changchun, China

Sources: China Mobile

4.6.2 Identification of factors affecting risk

(1) Identification of Personal Information Subject Interest

The interests of personal information subject generally include the interest of personality interests (personality dignity and freedom), economic benefits and convenience services. Mobile phone signaling big data can generate customer location information and activity track information, which involves personal privacy, has high sensitivity and significant value of personality interests; however, in space-time-behavior analysis, sharing mobile phone signaling big data is not significant for information subjects to obtain economic benefits and convenient services. Therefore, the important interest of personal information subject identified in this context is the interest of personality dignity and freedom (I_1).

(2) Identification of threats

Generally from the network environment, personal information processing flow, way of data sharing with third parties and other aspects to identify the threat of data sharing. The network environment of the information system dealing with personal information includes internal network or Internet. Different network environments face different threat sources and the threat of the information system connected to the Internet is higher. In view of the processing big data of mobile phone signaling is generally carried out in the private network, this threat may not be considered.

In specific application context, the most important threat (T_1) is the information

recognition of mobile phone signaling data in the process of personal information processing. The threats to the big data recognition of mobile phone signaling include trajectory identification, workplace-residence identification, accurate positioning to specific individuals, user portraits, etc., as well as high-frequency tracking or long-time monitoring of the whereabouts of information subjects.

The way of sharing data with third parties is also an important aspect that poses a threat (T_2). Confirm the data interaction mode between the mobile phone signaling data system of telecom operators and the third party data processing system. If the telecom operators only open part of the platform to the third-party, and the third-party processes the data on the physically isolated data system designated by the telecom operators and obtains the calculation results, the threat is mainly reflected in the code and plug-in of the third party, and the threat is low; if the telecom operators share the data by transmitting mobile phone signaling big data to the third party, the threat increases significantly It involves whether the third party receiving personal information strictly implements the contract agreement, whether the purpose of use will be changed, whether the storage time of personal information is minimized, whether it is timely deleted beyond the time limit, and whether the necessary security management measures are formulated and implemented according to the business security requirements.

(3) Identification of vulnerability

It mainly focuses on the vulnerability brought by the spatio-temporal attribute and data scale of mobile phone signaling big data in the specific context of urban planning based on space-time-behavior. Mobile phone signaling big data belongs to spatio-temporal big data, which has time and space dimensions, can reflect the spatio-temporal position, and is easy to be used by attackers, It is the first vulnerability (V_1). Using mobile phone signaling big data for space-time-behavior analysis, the number of data is often more than 10 million or even hundreds of millions, and the scale of information subject is more than 1 million. Once leaked, the consequences will be serious. It is the second vulnerability (V_2).

In general context (rather than individual case), considering the technical

strength and management ability of telecom operators, this research assumes that the mobile phone signaling big data has been anonymized before sharing. The border protection equipment has been deployed at the network boundary, the border protection strategy has been configured, and the data leakage prevention and intrusion prevention technical measures have been implemented. A complete network security incident warning, emergency response, notification and reporting mechanism has been established. Carry out regular security inspection, evaluation and penetration test for information system, and timely update patches and reinforce security. Have signed confidentiality agreements with relevant personnel engaged in personal information processing positions, and conducted background checks on a large number of personnel who have contact with sensitive personal information. Have carried out professional training and assessment of personal information security for relevant personnel in personal information processing positions. Have signed a binding contract and other documents with a third party, stipulating the purpose and method of processing personal information after it is transferred to the third party, as well as the data retention period and the processing method after the data exceeds the period. That is, the risks that may be caused by the above factors are not considered.

In summary, in the above application contexts, personal information subject interest I_1 faces two main threats: information transmission(T_1) and data transmission(T_2). The threat T_1 exploits the vulnerabilities are data spatio-temporal attributes V_1 and data scale V_2, and the threat T_2 exploits the vulnerability is data scale V_2. So there are three risks in personal information sharing.

4.6.3 Assignment of factors affecting risk

All kinds of factors are divided into five levels according to their degree, which are represented by 1-5 values from small to large. If the influence of factors is not significant, it will not participate in the risk calculation. (As shown in Table 4-2)

Personal information subject interest I_1:

The value of personality dignity and freedom is the core value of personal information. Let $I_1 = 5$.

Threat T_1:

In application context 1, taking the town as a unit for trajectory identification, the granularity is large and the accuracy is low. It's difficult to determine the identity of information subject. Let T_1=1.

In application context 2, taking the scale of 200m×200m as a unit to identify workplace and residence, as well as to identify the place of consumption and leisure. It can accurately locate the residential area, work place, daily consumption and leisure place, and it is very easy to identify the identity of the information subject, or even make a portrait of the information subject Let T_1=5.

Threat T_2:

The above two cases have not specified the specific sharing way of mobile phone signaling big data. For case comparison and analysis, it is assumed that the first application context is that the third party processes data on the physically isolated data system designated by the telecom operator and obtains the calculation results. Let T_2=1. And it is assumed that the second application context is that telecom operators share data by transmitting mobile phone signaling big data to the third party. Let T_2=3.

Vulnerability V_1:

Spatio-temporal attribute is the inherent attribute of mobile phone signaling big data. The positioning accuracy of mobile phone signaling big data depends on the base station density. Generally, the accuracy is about 200m, and the vulnerability is moderately controllable. Therefore, V_1 = 3 is set for both application contexts.

Vulnerability V_2:

The characteristics of mobile phone signaling big data are full-sample, dynamic and continuous, which will inevitably lead to massive data to be used. The number of data used in application context 1 is about 100 million, and the number of active users recorded is 1.3895 million. Although the number of data is not explained in application context 2, 1.6463 million people are identified from the research results and the data time span is 14 consecutive days, so the number of data should also exceed 100 million. Referring to the *Guidelines for Personal Information Security*

Impact Assessment, the scale of processing personal information exceeds 1 million people, its vulnerability is moderate. And the data has been anonymized, its vulnerability can be reduced as appropriate. Therefore, V_2=2 is set for both application contexts.

Table 4-2 List of assignment of risk factors under specific application contexts

	I	T	V
Application Context 1	I_1=5	T_1=1	V_1=3
			V_2=2
		T_2=1	V_2=2
Application Context 2	I_1=5	T_1=5	V_1=3
			V_2=2
		T_2=3	V_2=2

4.6.4 Risk calculation of personal information sharing

(1) Application context 1: The calculation process of the three risk values is similar. Now we take the personal information subject interest I_1, the threat T_1, and the vulnerability V_1 as an example to calculate and demonstrate.

① Calculating the possibility of the harm to the right and interest of personal information subject

Firstly, the possibility matrix of harm occurrence is constructed according to the empirical function $z_{ij}=x_i \times y_j$, as shown in Table 4-3. Substituting T_1=1 and V_1=3 into the matrix, the probability of harm was determined as 3.

$P_1(T_1, V_1)=P_1(1, 3)=3$

Table 4-3 Possibility matrix of harm

	Vulnerability Severity (V)	1	2	3	4	5
Threat Impact level (T)	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20
	5	5	10	15	20	25

Secondly, the possibility of harm is graded. As shown in Table 4-4, the possibility of harm is graded as "Less possible".

Table 4-4 Possibility level of harm

Possibility level of harm	Less possible	Rationally possible	Considerably possible
Possibility value of harm	1-5	6-15	16-25

② Calculating the severity of the harm to the right and interest of personal information subject

Firstly, the severity matrix of harm is constructed according to the empirical function $z_{ij}=x_i+y_j$, as shown in Table 4-5. Substituting $T_1=1$ and $I_1=5$ into the matrix, the severity of harm was determined as 6.

$S_1 (T_1, I_1)=S_1 (1, 5)=6$

Table 4-5 Severity matrix of harm

	Personal Information Subject Interest (I)	1	2	3	4	5
Threat Impact level (T)	1	2	3	4	5	6
	2	3	4	5	6	7
	3	4	5	6	7	8
	4	5	6	7	8	9
	5	6	7	8	9	10

Secondly, the severity of the harm is classified. As shown in Table 4-6, the severity of the harm is "Moderate harm".

Table 4-6 Severity level of harm

Severity level of harm	Minimal impact	Moderate harm	Severe harm
Severity value of harm	1-4	5-7	8-10

4.6.5 Risk level judgment

Application context 1: On the basis of comprehensive analysis of the possibility and severity of the harm to the right and interest of the personal information subject, according to the risk calculation model R (P(T, V), S (T, I)), and comparing with the risk judgment matrix (Figure 4-2), it is judged that the level of risk R_1 of personal information sharing is low risk.

Similarly, according to the above risk calculation process, it is judged that risk R_2 is low risk and risk R_3 is low risk.

To sum up, in the application context 1 "Using mobile phone signaling data to measure the hierarchical structure of urban system", the risk level of personal information sharing is low. Using mobile phone signaling data to measure the hierarchical structure of urban system, personal information can be used based on rational expectation rules.

Application context 2: Using the same method, it is judged that risk R_1 is high risk, risk R_2 is high risk, and risk R_3 is high risk. In the application context 2 "Using mobile phone signaling big data to study the spatial characteristics of urban activities and community differentiation", the risk level of personal information sharing is high risk. Using mobile phone signaling big data to study the spatial features of urban activities and community differentiation can not be based on rational expectation rule.

4.6.6 Discussion and suggestions

The rational expectation rule can only be applied when and only when all the risks judged are low risks. Obviously, in application context 2, it does not meet the conditions of reasonable expectation rule. The mobile phone signaling big data controller should significantly inform the information subject before sharing it in this context. Through the above case simulation, we can also find that sharing mode and grid cell size are the key points of the rational utilization of mobile phone signaling big data in space-time-behavior analysis. In application context 2, If the technical conditions and research accuracy permit, the risk can be reduced by optimizing the sharing mode and increasing the grid size to meet the applicable conditions of rational expected rule.

4.7 Chapter conclusion

Personal information includes the values of personality dignity, economic use, and public management. In the age of big data, stakeholders of personal information have become increasingly diverse. Sharing and making rational utilization of personal information on the premise of guaranteeing core interest of personal information

subject and balancing the relation among personal information protection, digital economic development and public interest maintenance become the intrinsic demand of the rapid development of economy and social. In the age of big data, the informed consent oriented traditional protection model has been not operable. Instead, the rule of rational expectation becomes a key option of personal information protection. The boundary of rational expectation can be judged by assessing the risk level of sharing personal information in specific context. If the risk assessed is at the level of low risk, the sharing and use of personal information in this context complies with the rational expectation rule; If the risk assessed is at the level of medium risk, it is necessary to take measures timely and actively to reduce the risk and reassess the risk; If the risk assessed is at the level of high risk, the rational expectation rule is not applicable, the personal information controller should significantly inform the information subject and obtain consent before sharing the personal information. If there are multiple risk points in the application context, when and only when each risk level judged must be low risk, the rational expectation rule can be applied. Namely, risk is tolerable but should be controlled in acceptable range of low risk.

Chapter 5 Rational Utilization of Personal Information in Smart Campus During COVID-19 Pandemic

5.1 Introduction

During the period of COVID-19 pandemic, many industries and businesses have been impacted, as well as the education of universities. Usually, universities will take two main measures, first is postpone school start date and conduct online education when the pandemic is severe; Second is increase efficiency in campus management and start offline education when the pandemic is slow down.

Smart campus comprehensively uses emerging information technologies such as IoT, mobile Internet, intelligent perception, big data, and knowledge management to fully perceive the physical campus surroundings, intelligently identify the learning, work situation and individual features of the teacher and student groups, and integrate the school physics Space and digital space are organically connected to create an intelligent and open education and teaching circumstances and a convenient and comfortable living circumstances for teachers and students, change the way teachers and students interact with school resources and environment, and realize personalized and innovative services based on people.

Personal information is helped to universities to ensure education and management quality during the period of COVID-19 pandemic. In smart campus, student personal information is necessary for all the activities of education and management. From the point of view of usage of big data in education, students' individual data and their learning activities as student personal information now are possible to be collected by education system and many sensors using ICT in university campus(Huang, Yang, et al., 2012), which will have great impact on dynamic teaching and learning interactions between faculty members and students (Nguyen and Williams, 2016). If the data related to students is stored in cloud system, it will greatly improve the convenience of teaching and management. Meanwhile, if student interaction recorded in a cloud system of Learning Management System

(LMS) can be used as real-time feedback to teachers in classroom, ICT will change the education style thoroughly (Kobayashi, Arai et al., 2017; Kim, Song et al., 2011). However, we can also image that the limitations of time schedule and classroom place probably can be removed if LMS carries out in a style of on-demand education, and students can access LMS when they need and it is not necessary to ask students for attending the classroom according to time schedule in future. Multi-method approach can be possible for dynamic teaching using LMS. For online and offline education methods, the usage of personal information is different.

The global spread of COVID-19 has been disrupting teaching plans and suspension of classes for more than 850 million students worldwide (Tinggui Chen, Lijuan Peng, et al., 2020). After the outbreak of COVID-19, universities campus were closed to prevent the virus spreading. To ensure that students acquire sufficient knowledge, many universities started to offer online course to students. From the aspect of study independence, there are two main types of online course, asynchronous online course and synchronous online course. Asynchronous online course refers to the education method that puts the produced learning materials and videos on the platform for students to learn independently. The advantages of asynchronous online course are low cost, more refined courses, courses can be edited and re-recorded, and meet the needs of students to watch them in fragmented time. The disadvantage is that it cannot be supervised and the completion rate is relatively poor. Students are hard to pay attention for more than an hour during asynchronous online course, and difficult to guarantee the learning effect. Synchronous online course means that both teachers and students need to attend classes at a designated time. Teachers and students enter the online classroom at the same time, and the teacher teaches in real time. In this process, students can communicate with the teacher in time. The advantage of synchronous online course is that teachers and students can interact, the learning effect can be supervised. Therefore, the learning effect will be better than asynchronous online course, especially for students who have poor self-control and are easily distracted. In China, universities often use Tencent Meeting, QQ/WeChat group video call, and DingTalk to give synchronous

online courses. These software were originally designed as online office meeting or group chat tools, sometimes cannot meet all the demands of online education. As for asynchronous online course, universities often choose i-Course (also called Chinese University MOOC), XuetangX, Zhihuishu and other massive open online courses platforms. Usually, these platforms cooperate with universities, students account in those platforms will also bind with their student ID of university.

With all the campuses closed, students can only acquire knowledge by online education, which causes some challenges. A survey of an university showed that students feel that online learning and classroom learning standards are not the same, they are anxious about online learning and disappointed at the graduation ceremony (Unger and Meiran, 2020). Besides, network fault, lack of training and self-learning consciousness were the main problems about online education. These problems caused students hard to adopt online learning, and doubt on the effectiveness of online education (Arora and Srinivasan, 2020). Although there are some difficulties and shortcomings about online education, students and teachers are constantly adapting and improving online education. A case study in Georgia indicate that the rapid change to online teaching has been successful, and the accumulated experiences can be used for future education (Basilaia and Kvavadze, 2020). A survey in China Southeast University shows that with the help of online education, about 50% of students believed that the planned teaching goals have been fully achieved, and 46% have basically achieved the goals(Sun and Tang, 2020).

To improve the quality of online education, personal information will inevitably be used. When students and teachers using online education software or platform, personal information will be required. The abuse of technologies increases the vulnerabilities of personal information,, which has lead to growing concern about issues of personal privacy among many people (Álvarez, Olmos, et al., 2002). The commercial utilization of personal information should be strictly monitored. Education strategy should more explicitly encourage the protection of online privacy, and the control of information disclosure behavior, then may consider the latent commercial and non-commercial purposes (Bryce and Klang, 2009). When the

epidemic of COVID-19 slowed down, the university campus continued to open, trying to combine offline teaching with online teaching. However, the campus is a densely populated area. In order to ensure the necessary social distance and track suspected infection cases, the campus has taken strict prevention and control measures, such as collecting students' health information and travel information.

While much studies have been carried out on online education and personal information respectively, but up to now few of them has dealt with how to rationally use personal information in online and offline education. This chapter is to investigate how personal information is reasonably used to balance the needs of teaching devices and services, guide students' good learning behavior and healthy life behavior, and ensure the quality of education and management in university during the COVID-19 Pandemic taking Fuzhou University as an example. For improving hybrid teaching method, we take Kanazawa University, as one of cases that use the LMS for e-learning, to discuss current approaches to implementing LMS for education activities based on student personal information in order to find out the obstacles of using LMS in a pilot course using ordinary classroom in smart campus.

5.2 Research approach

The study selected and collected the notices and policies of Fuzhou University from January 1st, 2020 to January 31st, 2021 during the COVID-19 pandemic. Criteria for selecting the notices and policies were as follows: (i) Notices and policies about postponement of school start date; (ii) Notices and policies about online education; (iii) Notices and policies about postponement of internship or graduation; (iv) Notices and policies about closed-off management over school; (v) Notices and policies about management of students and faculties back to campus. Then, we used questionnaire survey and interviewed teachers and students to obtain online education information of the School of Architecture and Urban-rural Planning of Fuzhou University. The course title, course code, course schedule, teacher's name, online education platform or software, QQ group number and URL of the online course were collected. After

that, we classify personal information types, target population, application and collecting methods to investigate how to use personal information to ensure education and management quality during the COVID-19 pandemic. In addition, we also investigated the views of teachers and students on epidemic prevention and control measures. At last, take Kanazawa University as an example, we use questionnaire survey method to investigate hybrid teaching activities, in order to explore classroom design needs when carrying out hybrid teaching in LMS.

5.3 Personal information in university education and management

5.3.1 Personal information used in online education and management

Table 5-1 shows the current application of personal information in online education and management. We extract types of personal information, target population, application of personal information, and the methods to get these personal information. We found that some information are used to register platform account, such as name, student ID, teacher ID, affiliation, and phone number. Some personal information are used to conduct and attend the class, such as the camera, microphone, screen, and log data. Those personal information are given by teachers and students. What's more, some universities will supervise and inspect online course by using student's online education platform account and password to log in.

Table 5-1 Current application of personal information in online education and management

Personal Information	Target Population	Application	Methods
1. Name 2. Student ID 3. Affiliation 4. Phone number	Students	Platform account registration	Input by studetns
1. Name 2. Teacher ID 3. Affiliation 4. Phone number	Teachers	Platform account registration	Input by teachers
1. Camera 2. Microphone 3. Screen 4. Log data	Teachers and students	Conduct/attend the class	Turn on by teachers and students
1. Account and password of online education platform	Students	Supervision and inspection of online course by university	Chosen and collect by university

5.3.2 Personal information used in offline education and management

Table 5-2 shows current application of personal information in offline education and management. Traffic data and health information of teachers and students are often used to determine whether they should quarantine or not, and when to return to the campus. These information are reported by online system or software, and usually required daily report. If there are suspected cases in campus, name, sex, residential ID number, phone number and house address should report to university. And then university will quarantine them and sent them to the hospital. When teachers and students enter the campus, they should provide traffic data, health information, and show the campus card, which contains name, and student ID or teacher ID. For students who want to leave the campus, they should report name, student ID, phone number, accompanies after leaving the campus and destination after leaving the campus.

Table 5-2 Current application of personal information in offline education and management

Personal Information	Application	Methods
1. Traffic data	Determine whether to return to campus or not;	Online report by teachers and students
2. Health information	Determine whether to quarantine or not; Determine when to return to campus	
1. Daily health information	Determine whether to quarantine or not	Online report by teachers and students;
		Check by staff
1. Name 2. Sex 3. Residential ID number 4. Phone number 5. House address	Quarantine and sent to the hospital	Check by staff
1. Traffic data 2. Health information 3. Name 4. Student ID 5. Teacher ID	Enter the campus	Check by staff
1. Name 2. Student ID 3. Phone number 4. Accompanies after leaving campus 5. Destination after leaving campus	Leave the campus	Online report by students

5.4 Discussion on the application of personal information in education and management during the COVID-19 pandemic

5.4.1 Personal information application in online education and management

5.4.1.1Current relationship of personal information in online education and management

Figure 5-1 shows the current relationship of personal information in online education and management, their application, and the purpose of why these personal information are used. We can see from the figure that there are two purpose of using personal information in online education, which are support the platform to realize online education. The other one is to support university to ensure the quality of education. This figure also shows that personal information like name, student ID, Teacher ID, affiliation, phone number, camera, microphone, screen, and log data are used to realize online education. Personal information like online education platform account and password are used to ensure the quality of education.

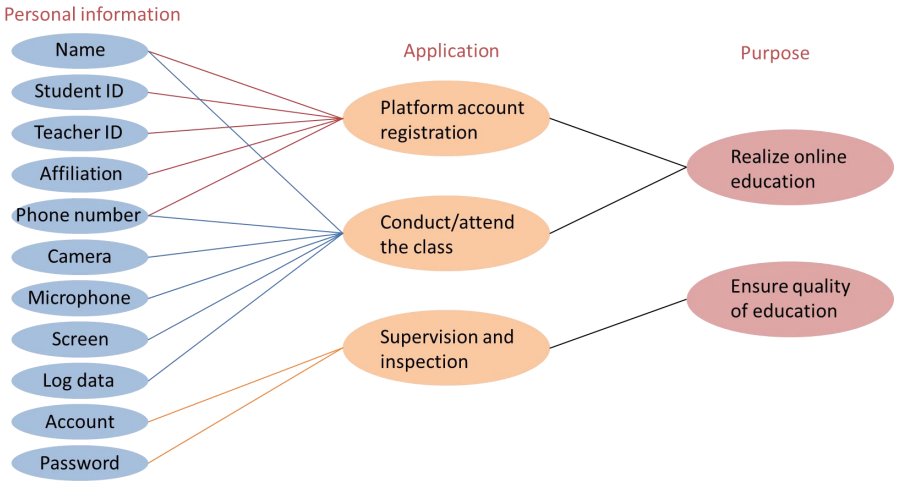


Figure 5-1 Relationship of personal information in online education and management

5.4.1.2 Problems of current online education and management

Although online education is very convenient during the COVID-19 pandemic, there some problems of current online education. Figure 5-2 and Figure 5-3 is the result of interview of Fuzhou University. Figure 5-2 shows the difficulties encountered by students in online education and management. Most students think being unable to concentrate, network issues and need to switch between too many online education platforms are the main problems. Other problems are insufficient self-learning ability, the online course is difficult, cumbersome teaching methods, lower classroom interaction, too much homework, and insufficient teaching materials.

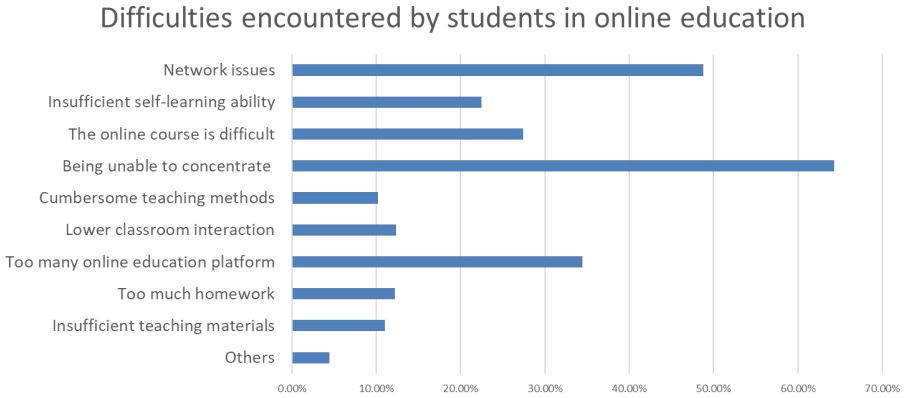


Figure 5-2 Difficulties encountered by students in online education

Figure 5-3 shows the difficulties encountered by teachers in online education. Difficult to know the learning status of students , lower classroom interaction and unfamiliar with online education platform are the main problems that teacher

encounter in online education. There are other problems, which are network issues, inadequate preview and review lessons, students are lack of focus, difficult to adjust the curriculum, difficult to handle emergencies and difficult to start teaching.

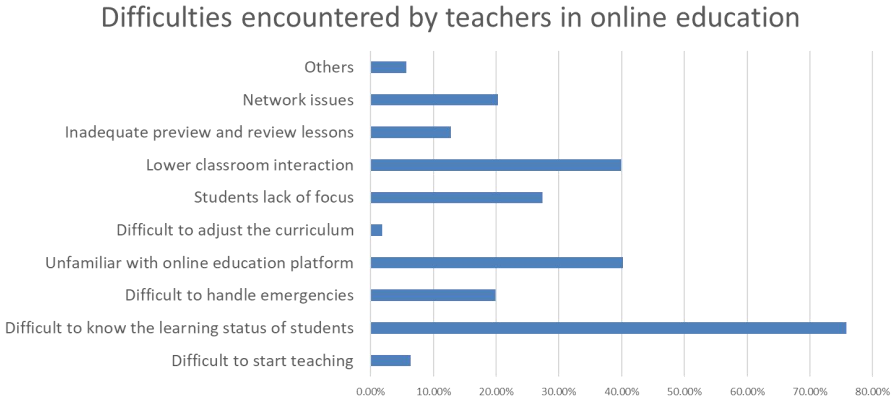


Figure 5-3 Difficulties encountered by teachers in online education

Except for technical problems, no effective supervision and inspection and the course is not attractive enough are the main reasons why students encounter these difficulties. Insufficient teacher-student interaction and unfamiliar with online education are the main reasons why teachers encounter these difficulties.

5.4.1.3 Recommended application of personal information in online education and management

Therefore, to solve these problems in online education, we proposed some recommended application of personal information. To improve the supervision and inspection in online education, usually, the platform can know you already attend online course by students' website log data. But sometimes, we cannot check if students are in front of the computer, or if students are browsing other websites. In this case, we can use camera data and screen data to supervise and inspect. Besides, to ensure the quality of education, improve the lesson preparation is also important. Through a survey of students, it is found that some students' family conditions are not very good and live in a remote village, which leads to poor network conditions. If teachers consider the needs of this part of students, they can add materials that can be downloaded by themselves in addition to the synchronous online course, which can improve this part of the problem. Or some homework assigned by teachers is not very

convenient to complete under some students' family conditions. If the teacher knows the situation of the students ' family (can be anonymous), the content of the homework can be changed. Students' interest and their past and current learning status can also help teachers to o improve the lessons. (As shown in Figure 5-4)

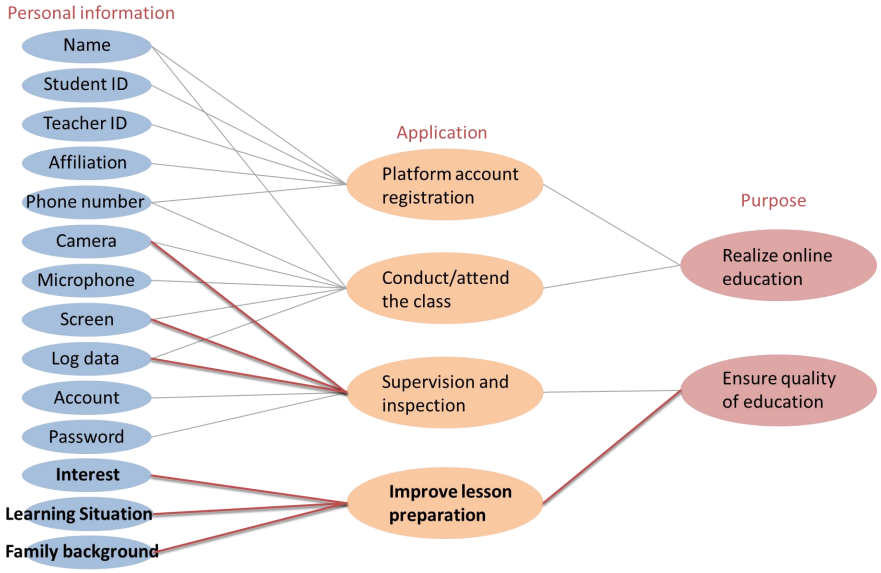


Figure 5-4 Recommend application of personal information in online education and management

5.4.2 Personal information application in offline education and management

In order to prevent and control the epidemic and maintain social distance in offline education, students are extra required to fill in health information daily by using mobile app, and the app must be positioned within the campus before it can be used.(As shown in Figure 5-5) When students leave campus, they must ask for leave from their tutors. When they go to high-risk areas, they must report in time and provide virus nucleic acid test report to prove that they are healthy. Students must show the "Health Code" (Figure 5-6) when they enter the campus, which integrates the students' personal identity information, health information and activity track information. If everything is normal, the code will be displayed in green. On the contrary, if there are unsafe factors, the code will be displayed in red.

Figure 5-5 APP for filling in health information

Figure 5-6 Health Code

5.4.2.1 Current relationship of personal information in offline education and management

Figure 5-7 shows current relationship of personal information in offline education and management. As we can see, the application of personal information is about whether to quarantine and sent to hospital, and go in and go out of the campus. The purpose of using personal information is only to prevent and control COVID-19 pandemic in the campus. However, the application of personal information in offline education is more than it in online education.

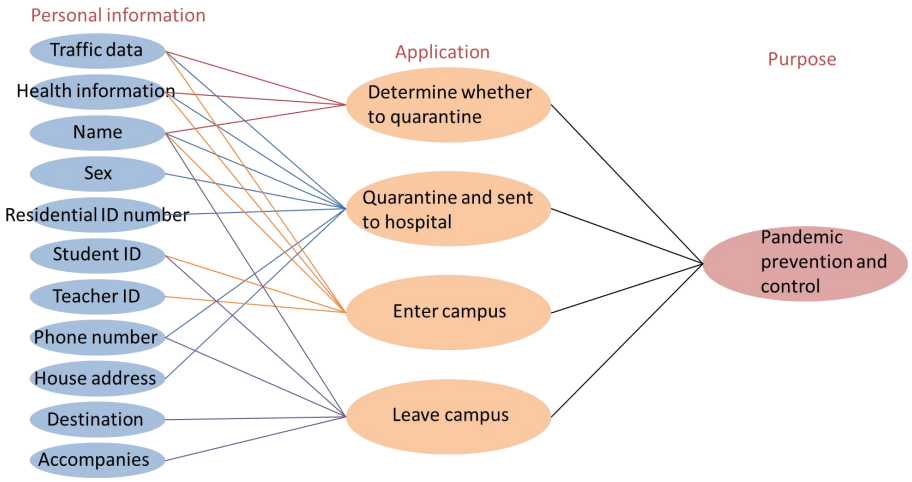


Figure 5-7 Relationship of personal information in offline education and management

5.4.2.2 Problems of current offline education and management

First is personal information is used in COVID-19 pandemic prevention and

control. They have been used to manage campus, such as determine whether and when for teachers and students to enter and leave the campus, or determine whether to quarantine or not. In China, based on the needs of public interest and epidemic prevention, personal information can be collected without informed consent. But in some other countries, this is not allowed, or the law has made strict restrictions on the collection of personal information in such cases. Second problem is most of personal information are collected manually and it will lead to the poor effect of the actual use. For example, there may be some delay, omission, falsification or concealment in reporting their traffic information or health information. Moreover, data collection and analysis are not efficient enough.

5.4.2.3 Recommended application of personal information in offline education and management

Figure 5-8 shows how we address those problems in offline education by proposing some recommended application of personal information. Same with online education, we can use students' interest, learning situation and family background (e.g. whether they can afford smart devices) to improve the lesson preparation to help ensure the quality of education. What's more, if we install card reader in every public room, and require people to check-in with their campus card, we can get the details of location information of each person in the campus. Therefore, we can do contact tracking in the campus, and help to determine whether someone should quarantine or not. Besides, students and teachers can make reservation online to apply the use of campus facilities such as meeting room, gym, library. If students want to sit in on a class, they should also make reservation in advance.

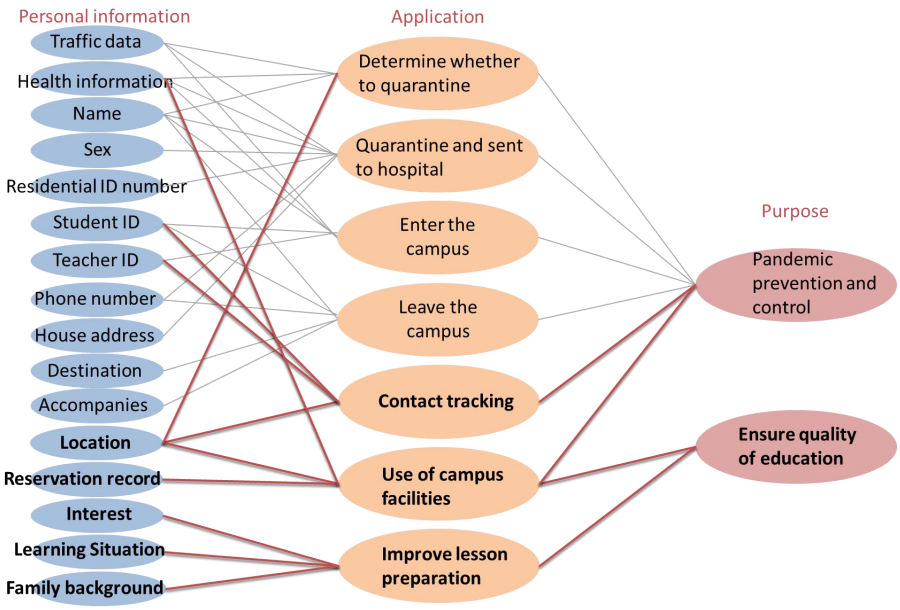


Figure 5-8 Recommend application of personal information in offline education and management

5.4.3 Personal information protection

The more personal information we use, the higher risk of personal information leakage will be. Therefore, we should take measures to protect personal information. Measures in online education and offline education have some differences. There are some measures about personal information protection in online education. First, if the online education platform or university want to use teachers and students personal information, they should have the informed consent and cannot shared the information to others, or disclosed to the public. Also, the personal information they collect only can be used for supporting online course or improving the quality of education. It can't be used for other purposes, like commercial advertising. Second, we should improve relevant laws and regulations. Because online education has just emerged in recent years, laws and regulations are not good enough. Some platforms or individuals may disclose users' personal information due to financial interest. Hence, there is an urgent need to improve the relevant laws and regulations of online education personal information protection. Therefore, it is necessary to improve relevant laws and regulations. Third is to improve the technologies on network security measures. Use technical methods to detect whether there is abnormal personal information acquisition and abnormal usage of personal information.

The other part is about personal information protection in offline education. First is same with online education, university should have the informed consent and cannot shared the information to others, or disclosed to the public. Second, personal information can be used reasonably based on the public interest in an emergency. We should notice that the emergency should stipulated by laws. Finally, university should set up supervision department to check if there is any misuse of personal information.

5.5 Hybrid teaching is the future trend: a practice of LMS in Kanazawa University

We can see from above that both online and offline education have their limitation. Therefore, combining online and offline education will benefit student education in the future. Online and Offline Hybrid Teaching are based on online open course resources, online teaching platforms and smart teaching tools. This teaching mode has a variety of teaching theories, teaching strategies, teaching methods and organization forms in school teaching to organically combine online teaching with traditional classroom. Hybrid teaching can make the best of massive open online courses and traditional classroom interaction. It expands the time and space of teaching and learning and solves various teaching contradictions caused by limited high-quality educational resources, limited space, and limited learning hours. It focuses on the personalized learning and diversified development of learners, and contributes to the frequent interaction between students and teachers, also between students each other. The pilot of online and offline hybrid teaching with LMS in Kanazawa University is a very meaningful attempt.

LMS can support teaching and learning, which is one kind of Smart Education System.(Shown as Figure 5-9) Generally speaking, the learning process could be separated into three stages: before class, in class and after class, which are preparation for a lesson, learning in class and review shown as Table 5-3. In the step of preparation of a lesson, PowerPoint files, e-Textbook and Video materials for lesson can be prepared by faculty member who take charge of the course. After class,

students read the e-Textbook, PowerPoint files for reviewing the teaching content and finish homework by Report System.

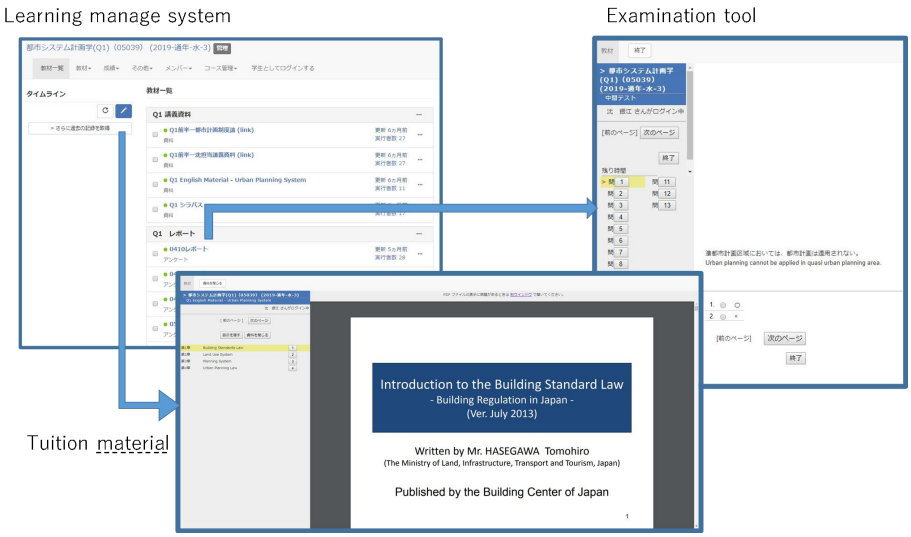


Figure 5-9 Learning Management System

Table 5-3 Learning Management System for faculty members and students

	Students' work	Teaching materials in LMS
preparation for a lesson	Reading textbook	e-Textbook system
		Video teaching materials
		Powerpoint files for course
Learning in classroom	Practice	Report system
	Attendance	Card reader system
	Listening	Powerpoint files for course
	Q&A	Question corner system
	Examination	Test system
Review	Reading textbook	e-textbook system
	Finishing HomeWorks	Report system
	evaluation of teaching	Questionnaire system

5.5.1 Rational use of student personal information in LMS

The essential condition of applying LMS is to collect student personal information including personal data and their learning activities using LMS. There is much student personal data that should be recorded in database for education management (Sinn, Kim, et al., 2019), such as students' name, telephone numbers, tutors' name, locations of the students, grades, registered courses, relating documents like "Survey of health status", "Diagnosis certificates of physical examination",

"Original copy of family situation", including all information of both students and the parents. Moreover, the learning activities like accessing time, academic records, attendance to classes and other are necessary to be saved in database of LMS.

However, there are many critical issues like whether the personal information can be shared to the third party without the individual consent, and how to define the limitations of providing concerning the specific personal information. In cases, even if the information subject agree to open his personal information, it still can not be provided beyond the scope of application. Even though it is relating to the schooling assistance procedures and so on, it must be used with caution, and student personal information should be limited only for smart education using LMS. Regarding the provision of students' personal information to LMS, recently there are strict online personal protection regulations towards the online personal information for online business management (Steppe, 2017). The university authorities should necessarily protect the personal information in all education activities using LMS. Japanese universities make the regulations of personal information protection based on the *Personal Information Protection Act*, making rules on the the object of personal information, the acquisition, protection and management of personal information, and sharing personal information to the third party when considering the design concept of LMS . (Higashi, Kasahara, et al., 2013)

5.5.2 Learning activities in classroom and in LMS

In the step of learning in class, students can register their attendance by Card Reader System, finish their practice during the class using Report System and join the examination using Test System. In the steps of preparation and review, students can use LMS for study. However, during the class in ordinary classrooms that only have conventional equipment such as shown in Figure 5-10 and 5-11, after students use their student cards to register their attendance, usage condition of the LMS is still limited for students besides of using screen to present teaching materials.

Figure 5-10 Devices in ordinary classroom

Figure 5-11 Ordinary classroom

Multi-mode hybrid teaching should be adopted to support the students' learning, which is a subject of LMS in smart education process. General speaking, a suitable way for using LMS in classroom, diversity of learning strategies, different learning styles are expected to boost performance and foster a classroom atmosphere. For considering if ordinary classroom is suitable for the teaching materials uploaded to the LMS, the teaching experiment has been conducted. In the new way of teaching using the LMS, including pre-learning, group work and individual work and Q&A chat were designed in the class time.(As shown in Figure 5-12)

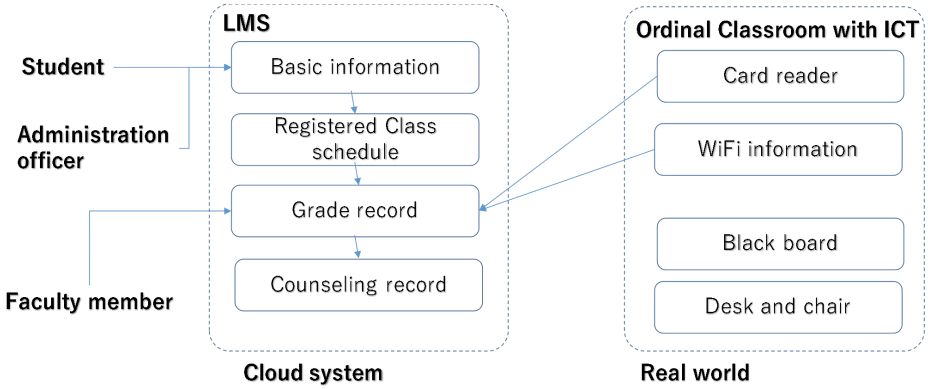


Figure 5-12 LMS and ordinary classroom

5.5.3 Pilot teaching practice of using LMS in ordinary classroom

Few faculty members use LMS to improve their education in courses because they must teach in the ordinary style of classroom even the university started to encourage faculty members to start pilot education in some course. The authority of Kanazawa University is planning to use LMS for improving the quality of education by the new education way suitable to LMS. For this, a project namely Pilot Teaching Practice has been started from 2018. Two courses in school of Earth Science and Civil Engineering were chosen as case study for teaching experiment.

One of two courses is Planning Process, which teaching faculty planned to use LMS for teaching experiment in order to find out if the ordinary style of class is suitable for the teaching way of LMS. There were 90 students in this class who were studying in the spring semester from April to July 2019 in their second academic year. The faculty member A who took charge of this class, chose one of lecture for teaching experiment. One teaching assistant and another faculty member B help main faculty member A to conduct this teaching experiment.

As required by the way of Pilot Teaching Practice, teaching materials should be uploaded to LMS firstly. For this, teaching materials include a video uploaded to YouTube, a PowerPoint file, an exercise web page with four questions have been prepared for students. Beside the teaching materials, a chat room is also prepared in the LMS for questions and answers between teachers and students as shown in Figure 5-13 to 5-15.

Students who registered for this course can watching the video as shown Figure 5-13 before the class. They have to finish the four question as excise during the time of class as shown in Figure 5-14. If they have question, they can ask via the Chat room as shown in Figure 5-15 during the class time and before and after class. Students are encouraged to gather the classroom and they can work on their assignment individually or as a group. In the new way of multiple teaching approach using the LMS, namely Active Learning Class (ALC) including pre-learning, group work, individual work and Q&A chat were designed in the LMS. For considering if ordinary classroom is suitable for the teaching materials uploaded to the LMS, the results of conducted teaching experiment has been discussed in next section.

Figure 5-13 Teachers' talking via YouTube

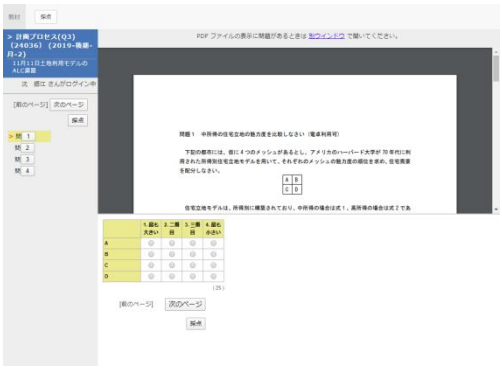


Figure 5-14 Exercises by individuals or groups

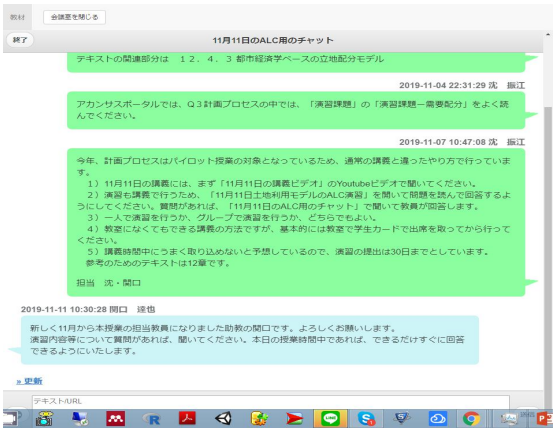


Figure 5-15 Q&A Chat room during the time of Pilot teaching class

5.5.4 Students' evaluation on Pilot Teaching Practice

As explained in the previous section, a teaching experiment has been carried out in the class of Planning Process scheduled on Nov. 11, 2019. A questionnaire to the students who joined the ALC class is prepared and students answered the questions

after the class. There are 81 students who are respondents to this questionnaire. By using LMS, the faculty members can check all students' activities regarding their ALC situations of this Pilot Teaching Practice because all of their activities recorded in the system. It is possible to communicate with students and teachers in real time for online teaching Q&A process.

5.5.4.1 Pre-learning

The first question is about pre-learning of the 81 students. 55 students (69% of all students) downloaded the teaching materials and conducted pre-learning using the LMS as shown in Figure 5-16.

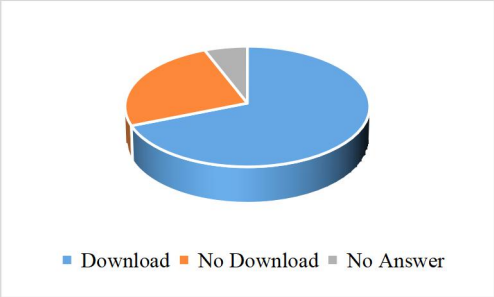


Figure 5-16 The student number who downloaded teaching materials for pre-learning

5.5.4.2 Pilot Teaching Practice

The new teaching way that is a multiple teaching approach, namely Pilot Teaching Practice includes group work for discussion and cooperation and individual work for exercises.

We ask students to express their own situation of ALC including group work and individual work through free description. As shown in Figure 5-17, totally 46 students responded that they can understand the content prepared in the pilot teaching practice by using teaching materials and the excise in the ALC class. But 35 of the 81 students answer that they fail to understand the content prepared in the class as shown in Figure 5-17. For ALC including group work and individual work, there are 15 students who like the new way of teaching because they can discuss with each other, and confirm with classmates for finding the solution of the question in excise by group cooperation and discussion to support individual work of excise. There are 7 students who said that the new teaching is difficult for them to understand and they

like the conventional teaching way instead of the pilot teaching practice. However, there were no any questions in the Q&A chat room system, which was probably ignored by students because of the busy time for finishing the individual work.

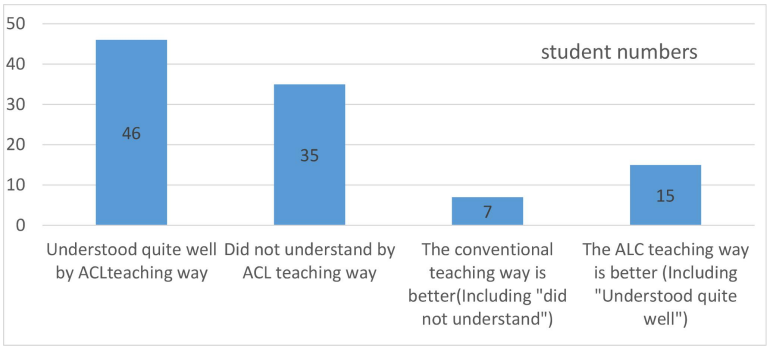
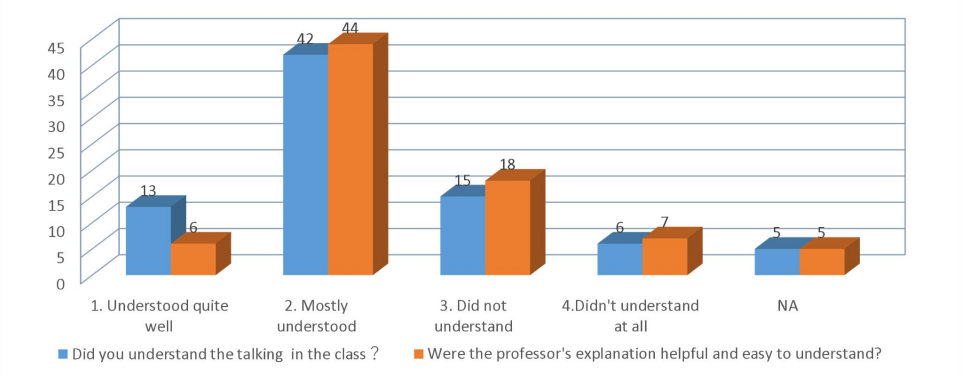


Figure 5-17 Understanding and the evaluation on Pilot Teaching Practice

5.5.4.3 Comprehensive evaluation to the pilot teaching practice

As shown in Figure 5-18, the satisfaction degree of understanding of the content prepared in the excise, there are 13 students who can fully understood how to find the solution of the excise designed in the practice, and 42 students who can almost understood how to complete the excise work. There are 21 students who campaigned that it is very difficult to find the solution of the excise work. Regarding the explanation of faculty member using video, 50 students said that they can understand, 25 students campaigned that they are difficult to understand from the prepared video.

As a result, we can conclude that the Pilot Teaching Practice is successful in our teaching experiment and most of students expect the new way of teaching can be put into the future class instead of conventional teaching style.



Blue: Comprehension of class content Orange: The clarity of the faculty's explanations

1: High 2: Somewhat High 3: Somewhat Low 4:Low NA: No answer

Figure 5-18 Comprehensive evaluation

5.5.5 Students' learning activities in their prefer spaces for pilot teaching practice

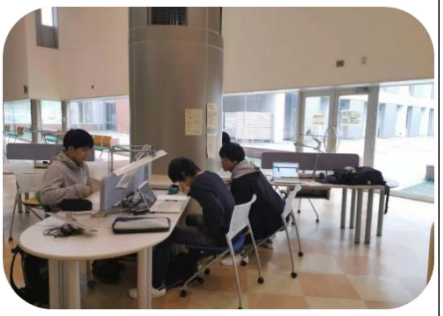
In the section 5.5.4, we can understand the Pilot Teaching Practice is preferred by most of students. By using LMS, when interview with faculty members, we make clarified that the faculty members can check all students' activities recorded in the system and can communicate with them in real time no matter that the students and faculty members are in the ordinary format classroom or not.

However, the ordinary style of classroom shown in Figure 5-19 is not suitable for students' activities in the Pilot Teaching Practice. It is very difficult for students to conduct group work for discussion and cooperation.

Figure 5-19 Pilot teaching practice in ordinary style classroom

1)Teachers' talking

2)Group wok for discussion



3)Group wok for cooperation

4)Individual exercises

Figure 5-20 Prefer spaces for students for group work and personal work using LMS

As shown in Figure 5-20, some of the students went out of classroom for finding

the spaces for group work, where discussion and cooperation was done more comfortable and freely. However, when group work of ALC style was encouraged by university authority, it is difficult to conduct many ALCs at the same time due to the limitation of free spaces in the building.

Moreover, in the pilot classes, many students brought their laptop PCs to the classroom. Certainly, their laptop PC allowed students to conduct location-independent works. However, if the classroom has the suitable equipment for conducting the ALC such as movable desks or internet accessibility for each student, their works would go smoothly.

Thus, the faculty members can check all students' activities recorded by using LMS and can communicate with them in real time no matter that the students and faculty members are in the ordinary format classroom or not. Students can choose their own way to study, such like group work, individual excise, and they can choose their prefer spaces for the kind of pilot class. However, there are limitations to organize the pilot education program in ordinary classroom for the multi-teaching approaches using LMS, particularly for students' activities. Accordingly, the design of classroom space faces the challenges from LMS for improvement the quality of education, and a new style of classroom that can be used for group work, individual excise is necessary.

5. 6 Chapter conclusion

In smart campus, during the period of COVID-19 pandemic, universities may use personal information rationally to balance the needs of teaching devices and services, guide students' good learning behavior and healthy life behavior, ensure education and management quality. Usually, universities will postpone the opening date of campus and conduct online education when the pandemic is severe, will increase efficiency in campus management and start offline education when the pandemic is slow down. In current online education, the rational use of personal information will effectively improve the teaching quality. In current offline education,

measures taken to prevent and control the pandemic need a lot of personal information, such as travel schedule, travel purpose, health information and so on. Based on crucial public interests, such as COVID-19 pandemic prevention, universities can make rational use of students' personal information. But because it involves personal privacy, it is necessary to strengthen the personal information protection both online and offline education. With the help of personal information, and the combination of online and offline education, the use of public teaching devices and services can be planned in real time to achieve the balance between supply and demand.

Chapter 6 Conclusions

6.1 Conclusions

In this dissertation, through a comparative study of the laws and regulations related to personal information protection in major countries and regions in the world, the issue of personal information protection and rational utilization in space-time-behavior analysis in the era of big data is discussed. This research analyzes the dilemma faced by the basic principle of "informed consent" in the era of big data, and points out the conflict between the current anonymization protection way of data sharing and the usage method of personal information in space-time-behavior analysis. Then, the theory of "rational expectation" is introduced, and the matrix method is applied to assess the risk of personal information utilization in specific context. The judgment standard for personal information protection and utilization based on "rational expectation" in space-time-behavior analysis is proposed, so as to achieve the balance of interests of relevant stakeholders and realize the protection and rational utilization of personal information in the age of big data. An example is given to illustrate how universities use personal information to guide students' behavior and realize the smart campus planning and management during COVID-19. Through the above research, the conclusions are as follows:

First, the concepts of personal information, personal data, and personal privacy are both related and different. From the legislative practice of various countries, personal information and personal data are similar concepts, and their denotation and connotation are almost the same. In the legislative mode of case law of common law system, personal information and personal privacy are basically the same, generally more use the expression of personal privacy. In the legislative mode of the statute law of the civil law system, it is generally believed that personal information and personal privacy are different, and there is an inclusive relationship between them, that is, the category of personal information includes personal privacy, and personal privacy is a subset of personal information. Whether a type of information belongs to personal

information can be judged as per the following three features: identifiability, idiosyncrasy, relativity, and the information with anyone of the three features should be judged as personal information. The personal information protection framework of Japan and China are basically similar to those of European and American countries. Informed consent is the basic principle of information protection all over the world. However, in the age of big data, information overload, status asymmetry, data explosion and rapid transmission are challenges to the principle of informed consent. The common law countries represented by the U.S. more focus on the use of personal information to promote the rapid development of the data industry, while the continental law countries represented by the EU more focus on the protection of personal information and are cautious about the in-depth development and utilization of data. However, the common trend of legislation is to seek a balance between personal information protection and rational utilization. The protection of personal information in Japan has its own style. It uses the concepts of personal information and personal data at the same time, and strictly protects "special care-required personal information" according to the sensitivity of information. Although the legislation of personal information protection in China started late, it has rapid and flexible progress with the late-development advantage, which not only promotes the fast expansion of big data industry, but also inevitably produces some hidden dangers.

Second, data resource has become an important factor of production, and has been widely used in all kinds fields of economy and society in the era of big data. The sharing and usage of spatio-temporal big data puts forward new thinking, new technique and new solution for urban planning, and also brings a new controversy about personal information protection and rational utilizstion. Mobile phone signaling big data is a kind of classic spatio-temporal big data, which can identify the trajectory of users and belongs to sensitive personal information. In people-oriented urban planning, we should use spatio-temporal big data to study the spatio-temporal features of people behavior track to build a fundamental analytical framework of "space-time-behavior". Thus, even though it is anonymized, mobile phone signaling big data will still display the user's position information. That is to say, anonymization

rule is not suitable for the sharing of mobile phone signaling big data in the space-time-behavior analysis. From the practice of China's urban planning, we can see that only depending on "anonymization" method to share and use mobile phone signaling big data, there are serious risks of infringing personal privacy and even causing the loss of personal property of the information subject. According to the current laws, in the space-time-behavior analysis, the sharing and use of sensitive personal information such as mobile phone signaling big data should get the informed consent of the information subject. However, in the age of big data, the principle of informed consent is facing difficulties in the application of spatio-temporal big data, which needs to be improved by other rules.

Third, personal information includes the values of personality dignity, economic use, and public management. In the age of big data, stakeholders of personal information have become increasingly diverse. Sharing and making rational use of personal information on the premise of guaranteeing core interest of personal information subject and balancing the relation between personal information protection, digital economic development and public interest maintenance become the intrinsic demand of the rapid development of digital economy. In the age of big data, under the context of massive and rapid data sharing, the informed consent oriented traditional protection model is facing difficulties, especially in space-time-behavior analysis, which needs a large amount of dynamic data, to fulfill the obligation of informed consent one by one seems to be not operable. Instead, the rule of rational expectation becomes a key option of personal information protection. The boundary of rational utilization can be judged by assessing the risk level of sharing personal information in specific context. Namely, risk is tolerable but should be controlled in acceptable range of low risk. Matrix method can be used to evaluate the risk of personal information sharing. If the risk is at a low level, the sharing and use of personal information in this context is in line with rational expectations. If the assessed risk is at the medium risk level, it is necessary to take timely and active measures to reduce the risk and re-evaluate the risk. If the assessed risk is at a high risk level, the rule of rational expectation is not applicable, and the personal

information controller must issue a major notice to the information subject before sharing personal information. In this case, data sharing can only be carried out with the explicit consent of users. If there are multiple risk points in the application context, the rational expectation rule can be applied only when each risk level judged must be low risk. Based on the rational expectation rule, we can achieve the balance of interests among personal information protection, digital economic development and public interest maintenance, so as to coordinate the promotion of digital innovation, economic development and social progress, and realize the unity of effective protection and rational utilization of personal information.

Fourth, under the influence of COVID-19 pandemic, universities may use personal information rationally to balance the needs of teaching devices and services, guide students' good learning behavior and healthy life behavior, ensure education and management quality in smart campus. Usually, universities will postpone the opening date of campus and conduct online education when the pandemic is severe, will increase efficiency in campus management and start offline education when the pandemic is slow down. In current online education, the rational use of personal information will effectively improve the teaching quality. In current offline education, measures taken to prevent and control the pandemic need a lot of personal information, such as travel schedule, travel purpose, health information and so on. Nevertheless, if increasing the collection and use of personal information, it will also face the problem of balancing personal information protection and rational utilization. Based on crucial public interests, such as COVID-19 pandemic prevention, universities can make rational use of students' personal information. With the help of personal information and the combination of online and offline education, the use of public teaching devices and services can be planned in real time to achieve the balance.

6.2 Legislative proposals

Law originates from life and is determined by specific social material conditions. With the fast expansion of information technology revolution, the lag of personal

information legal protection in the era of big data has become increasingly prominent. It will be a long-term and challenging work to improve the laws and regulations of personal information protection.

First, authorizes independent third parties in the form of legislation to conduct risk assessment on the application contexts of personal information. In the age of big data, the protection of personal information is no longer a simple negative defense of personality rights, but the combination of protection and rational utilization. Its focus is to protect the self-determination right of personal information, which includes not only the protection of personal right and interest, but also the necessary control and disposal of property rights and interests. At the same time, we should also fully consider the role of personal information as a data resource and production factor in promoting social and economic development. There is an interest game between personal information protection and data industry development. Because of the absence of relevant laws and regulations, a lot of data lying in the "data warehouse" occupy storage resources, but can not be effectively used. Authorize independent third parties especially industry associations through legislation to conduct risk assessments on the application contexts of personal information, use the rule of rational expectation to improve the principle of informed consent, construct a context-aware ecosystem to protect and rationally use personal information. American *Consumer Privacy Bill of rights Act of 2015（Draft）* is a useful attempt.

Second, allows the use of personal information based on public interest (such as epidemic prevention) through legislation. From the perspective of dialectics, public interest and personal interest are interdependent and unified. Public interest is relative, and personal interest is absolute. Public interest is composed of personal interest and embodied in the actual interests of most people.. The existence of public interest is based on the existence of personal interest. The realization of public interest is a powerful guarantee for the realization of personal interests. In order to meet the needs of public interest, some countries have legislated to authorize public authorities to collect and process personal information without the informed consent of the information subject. Some countries use technologies such as mobile phone signaling big data to track the activity trajectory of virus infected patients and their close contacts, and have achieved obvious prevention results, controlling the spread of the epidemic In a relatively short time. However, due to the different understanding of

public interest and different legal value orientation in other countries, the law does not authorize corresponding technical measures. In order to protect the basic human rights of life and health, it is recommended that various countries legislate to use personal information based on the needs of public interest such as epidemic prevention and control. It must be clear that once the public interest needs to be defined by law, information collection and use behavior must follow the provisions of the law and comply with the legal procedures, and a third-party supervision mechanism should be introduced to avoid abuse of power by public authorities.

Third, plays the roles of industry self-discipline fully to achieve multi-level comprehensive protection. It's necessary to formulate special laws and regulations to unify the principle and rule of personal information protection, meanwhile, play the role of industry self-discipline to formulate industry self-discipline norms according to the characteristics of the industry. The two complement each other in order to play the best protective role. Industry self-discipline norms are internal binding documents such as standards within the industry. Through mutual supervision among members within the industry, self-management of personal information protection in a specific industry can be realized. At present, the best country to use the industry self-discipline mode is the United States. The United States has always advocated industry self-discipline for the processing of personal information in the private field. The establishment of industry self-discipline norms can avoid the "one size fits all" of legal provisions, can meet the special needs of the industry's personal information protection, and is easy to be recognized by the majority of the industry in the same field, avoid the rule failure caused by the unified legislative model, and make up for the defects of the legal protection of personal information. For instance, private certification organizations in the United States, such as BBB online and Trustee, conduct third-party certification for personal information protection, which is also a typical model of industry self-discipline. In the age of big data, the balance between personal information protection and the development of digital economy should be a trend of data legislation; Strengthening the self-discipline of the industry, introducing independent third-party institutions for evaluation, and strengthening the supervision of the government at the level of law formulation and implementation should become an effective path for the protection and rational use of personal information.

6.3 Further research

This dissertation mainly from the perspective of law to analyze the protection and rational utilization of personal information. However, the understanding of the value of personal information is also influenced by cultural traditions, religious beliefs and social values, although these effects have been more or less reflected in the legislation. In different countries, there are differences in cultural traditions, religious beliefs, and social values, and the willingness to use personal information for value exchange to obtain convenience is also different, as well as the understanding of the government's role in personal information protection, resulting indifferent sensitivity to the same personal information and different understanding of the rational use of personal information. And this will affect the risk assessment of personal information utilization and the judgment of rational expectation. In the future research, we will consider more factors outside the law to build a more perfect the context-aware system.

In addition, with the continuous advancement of information technologies in the age of big data, the comparison and mining of ordinary personal information obtained in different ways may generate sensitive personal information and affect the protection and rational use of personal information, which must be fully considered in future research.

Publications and Conference

1. Yong LIN, Xiao TENG, Zhengjian SHEN. (2019). Comparative Perspectives on Personal Data Protection System for Smart City between China and Japan， *Proceedings of International Conference 2019 on Spatial Planning and Sustainable Development*, August 30th–September 1st, 2019, Chiba University, Japan.

2. Yong LIN, Zhenjiang SHEN, Xiao GUO, Xiao TENG. (2021). How Universities Use Personal Information to Ensure Education and Management Quality During the COVID-19 Pandemic：A Case Study of Universities in Fujian, China, Proceedings of International Virtual Conference 2020 on Spatial Planning and Sustainable Development, February 6-7th, 2021. https://www.spsdcommunity.org/spsd2020-vc/

3. Yong LIN, Zhenjiang SHEN, Xiao TENG. (2021). Review on Data Sharing in Smart City Planning Based on Mobile Phone Signaling Big Data From the Perspective of China Experience: Anonymization VS De-anonymization, *International Review for Spatial Planning and Sustainable Development*, Vol. 9(2):76-93. https://doi.org/10.14246/irspsd.9.2_76 (ESCI, SCOPUS)

4. Yong LIN, Zhenjiang SHEN, Xiao TENG. (2021). Personal Information Protection and Interest Balance Based on Rational Expectation in the Era of Big Data - a Case on the Sharing of Mobile Phone Signaling Big Data in Smart City Planning, *International Review for Spatial Planning and Sustainable Development*, Expected January 2022, 20 pages. (ESCI, SCOPUS) (Accepted)

5. Xiao GUO, Zhenjiang SHEN, Xiao TENG, Yong LIN. (2021).Using Web Data Scraping to Reveal the Relationship between AI product and Room Layout, *Design and Technological Applications in Sustainable Architecture - The perspective of China, Japan, Singapore and Thailand*, Springer, 13 pages. (In press)

References

Abul O, Bonchi F, Nanni M. (2010). Anonymization of moving objects databases by clustering and perturbation, *Information Systems*, Vol.35(8):884-910. https://doi.org/10.1016/j.is.2010.05.003

Álvarez JAT, Olmos A, Piattini M. (2002). Legal requirements reuse: a critical success factor for requirements quality and personal data protection, *Proceedings IEEE Joint International Conference on Requirements Engineering*, p95-103.

Arora AK, Srinivasan R. (2020). Impact of pandemic COVID-19 on the teaching–learning process: A study of higher education teachers, *Prabandhan: Indian journal of management*, Vol. 13(4):43-56. https://doi.org/10.17010/pijom/2020/v13i4/151825

Baek YM, Bae Y, Jeong I, Kim E, Rheed JW. (2014). Changing the default setting for information privacy protection: What and whose personal information can be better protected?, *The Social Science Journal*, Vol.51(4):523-533. https://doi.org/10.1016/j.soscij.2014.07.002

Bart S, Bart C, Simone H. (2014) The crisis of consent: how stronger legal protection may lead to weaker consent in data protection, *Ethics and Information Technology*,Vol.16(2):171-182. https://doi.org/10.1007/s10676-014-9343-8

Basilaia G, Kvavadze D. (2020). Transition to online education in schools during a SARS-CoV-2 coronavirus (COVID-19) pandemic in Georgia, *Pedagogical Research*, Vol. 5(4). https://doi.org/10.29333/pr/7937

BECKER RA, CACERES R, HANSON K, et al. (2011). A Tale of One City : Using Cellular Network Data for Urban Planning, *IEEE Pervasive Computingm*, Vol.10(4): 18-26. https://doi.org/10.1109/MPRV.2011.44

Benreguia B, Moumen H, Merzoug MA, (2020). Tracking COVID-19 by Tracking Infectious Trajectories, *IEEE Access*, Vol.8:145242 - 145255. https://doi.org/10.1109/ACCESS.2020.3015002

BOSHE P. (2015). Data privacy law: An international perspective, *Information & Communications Technology Law*, Vol.24(1): 118-120. https://doi.org/10.1080/13600834.2014.996324

Brandeis LD . (2014). *The Right to Privacy*, Peking：Peking University Press.

Bryce J, Klang M. (2009). Young people, disclosure of personal information and online privacy: Control, choice and consequences, *Information security technical report*, Vol. 14(3):160-166. https://doi.org/10.1016/j.istr.2009.10.007

Carlo R, Dennis F, Maria PR, et al. (2006). Mobile Landscapes: Using Location Data from Cell Phones for Urban Analysis, *Environment and Planning B Planning and Design*, Vol.33 (5): 727-748. https://doi.org/10.1068/b32047

Chai Yanwei, Shen Yue, Chen Zifeng. (2014). Towards Smarter Cities: Human-oriented Urban Planning and Management Based on Space-Time Behavior Research, *Urban Planning International*, Vol.29 (6): 31-37.

CHEN R, FUNG B C M, Mohammed N, et al. (2013). Privacy-preserving trajectory data publishing by local suppression, *Information Sciences*, Vol. 231(9): 83-97. https://doi.org/10.1016/j.ins.2011.07.035

Chen Zhenyu, Zhang MinFu, YanyanZhang, et al. (2017). A User De-Anonymization Attack Method for Trajectory Data Publishing, *Journal of Information Securyity Research*, Vol.3(10):902-912. https://doi.org/10.3969/j.issn.2096-1057.2017.10.005

Chen, T, Peng, L, et al. (2020). Analysis of user satisfaction with online education platforms in China during the COVID-19 pandemic, *Healthcare*, Vol. 8(3). https://doi.org/200. 10.3390/healthcare8030200

Chik WB. (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform, *Computer Law & Security Review*, Vol.29(5): 554-575. https://doi.org/10.1016/j.clsr.2013.07.010

Choi Hanbyul, Park Jonghwa, JungYoonhyuk. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, Vol.81:42-51. https://doi.org/10.1016/j.chb.2017.12.001

Dai Xin. (2020). Information Governance in "Pandemic Control State":Practices and Ideas, *Beijing Cultural Review*, (5):86-94. http://d.wanfangdata.com.cn/periodical/whzh202005010

Daniel R, John DA. (2007). A Personal Information Auction: Measuring the Differential Value of Privacy, // *AMCIS 2007 Proceedings*, 206, Keystone, CO, USA. https://aisel.aisnet.org/amcis2007/206

Ding Xiaodong. (2018). What is Data Rights? Data Privacy through EU's General Data Protection Regulation, *Journal of the East China University of Politics & Law*, Vol.21(4):39-53 http://dx.chinadoi.cn/10.3969/j.issn.1008-4622.2018.04.005

Dong Yulan, Pi Dechang. (2018). Novel Privacy-preserving Algorithm Based on Frequent Path for Trajectory Data Publishing, *Knowledge-Based Systems*, Vol.148:55-65. https://doi.org/10.1016/j.knosys.2018.01.007.

Ersoy EC. (2019). Examining Turkish law on data protection, *Computer Fraud & Security*, Vol.2019(9): 9-11. https://doi.org/10.1016/S1361-3723(19)30095-8

Fan Wei. (2016). Reconstructing the Path to Personal Data Protection, *Global Law Review*, Vol.38(5):92-115. http://dx.chinadoi.cn/10.3969/j.issn.1009-6728.2016.05.007

Gao Fuping. (2018). Personal information protection: from personal control to social control, *Chinese Journal of Law*, Vol.40(3):84-101.

HAN Xuzhi. (2018). The concept of personal information in legal dogmatics angle: Focusing on Article 76(5) of the Cybersecurity Law, *Journal of Chongqing University (Social Science Edition)*，Vol.24(2) : 154-165. http://doi.org/10.11835/j.issn.1008-5831.2018.02.013

HIGASHI A, KASAHARA Y, TAKATA Y，FUTATSUGI M, MATSUHIRA T, MORI Y. (2013). Design Concept and Operational Statistics of Portal System (Acanthus Portal) in Kanazawa University, A*cdemic Information Processing Environment Research*, p23-34. http://hdl.handle.net/2297/36056

Hon WK, Millard C, Walden I. (2011). The problem of "personal data" in cloud computing: what information is regulated?—the cloud of unknowing, *International Data Privacy Law*, Vol.1(4):211-228. https://doi.org/10.1093/idpl/ipr018

Horie S, Sasaki N, Kawase Y, Nagano C, Tsutsui T. (2006). Handling of workers' health information by employers in compliance with Personal Information Protection Law in Japan, *International Congress Series*, Vol.1294:205-208. https://doi.org/10.1016/j.ics.2006.01.059

Huang RH, Yang JF, Hu YB. (2012). From digital to smart: The evolution and trends of learning environment, *Open Education Research*. Vol.18(1):75–84. https://doi.org/10.13966/j.cnki.kfjyyj.2012.01.009

James WQ. (2004). The Two Western Cultures of Privacy:Dignity versus Liberty, *Yale Law Journal*, Vol.113(6):1151-1221. https://doi.org/10.2307/4135723

Jin Ping, Chen Ming, Sun Zhihao. (2018). Urban land use functional area identification method based on mobile phone signaling data, *Information & Communications*, (1):268-270. http://dx.chinadoi.cn/10.3969/j.issn.1673-1131.2018.01.133

Kim S, Song SM, Yoon YI. (2011). Smart learning services based on smart cloud computing, *Sensors*, Vol.11(8):7835–7850. https://doi.org/10.3390/s110807835

KOBAYASHI T, ARAI K, SATO H, TANIMOTO S, KANAI A.(2017). An Application Framework for Smart Education System Based on Mobile and Cloud Systems, *IEICE*, Vol.E100(10):2399-2410. https://doi.org/10.1587/transinf.2016OFP0001

Li Jian. (2014). How do telcos mine the "Gold Mine" of big data, *China Telecommunications Trade*, (3):82-83. http://dx.chinadoi.cn/10.3969/j.issn.1671-3060.2014.03.032

Liu Jinrui. (2017). *PERSONAL INFORMATION AND RIGHTS SYSTEM:THE DILEMMA AND FUTURE OF RIGHT TO INFORMATION SELF-DETERMINATION*, Pekin:Law Press·China.

Loideain NN, Adams R. (2020). From Alexa to Siri and the GDPR: The gendering of Virtual Personal Assistants and the role of Data Protection Impact Assessments, *Computer Law & Security Review*, Vol.36,

No.105366. https://doi.org/10.1016/j.clsr.2019.105366

Long Weiqiu. (2017). On the Construction of New Data Property and its System Structure, *Tribune of Political Science and Law*, Vol.35(4):63-77

Long Ying, Zhou Yin. (2016). Quantitative Evaluation on Street Vibrancy and Its Impact Factors：A Case Study of Chengdu, *New Architecture*, (1): 2-57. http://dx.chinadoi.cn/10.3969/j.issn.1000-3959.2016.01.009

LU Zhenbo, LONG Zhen, YU Qihang. (2019). Analysis on the Job-housing Spatial Distribution and Commuting Characteristics of Kunshan City Based on Cellular Signaling Data, *Modern Urban Research*, (3): 50-55. http://dx.chinadoi.cn/10.3969/j.issn.1009-6000.2019.03.007

Lv Binbing. (2021). The Consent Dilemma of Personal Information Protection and Its Solution, *Studies in Law and Business*, Vol.38(2):87-101. http://dx.chinadoi.cn/10.16390/j.cnki.issn1672-0393.2021.02.007

Machida M, Nakamura I, Saito R, Nakaya T, Inoue S. (2020). Changes in implementation of personal protective measures by ordinary Japanese citizens: A longitudinal study from the early phase to the community transmission phase of the COVID-19 outbreak, *International Journal of Infectious Diseases*, Vol.96:371-375. https://doi.org/10.1016/j.ijid.2020.05.039

Manfredini F, Pucci P, Tagliolato P. (2014). Toward a Systemic Use of Manifold Cell Phone Network Data for Urban Analysis and Planning, *Journal of Urban Technology*, 21(2): 39-59. https://doi.org/10.1080/10630732.2014.888217

Mantelero A. (2017). Regulating Big Data. The Guidelines of the Council of Europe in the Context of the Europe - an Data Protection Framework，*Computer Law ＆ Security Review*，Vol. 33(5):584-602. https://doi.org/10.1016/j.clsr.2017.05.011

McDonald AM, Cranor LF, (2008). The Cost of Reading Privacy Policies, *I/S: A Journal of Law and Policy for the Information Society*, Vol.4:563

Mendelson D, Mendelson D. (2017). Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework, *Ethics, Medicine and Public Health*, Vol.3(1):37-55. https://doi.org/10.1016/j.jemep.2017.02.005

Narayanan A, Shmatikov V. (2008). Robust de-anonymization of large sparse datasets, //*2008 IEEE Symposium on Security and Privacy (sp 2008)*, Oakland, California, USA, P111-125. https:/doi.org//10.1109/SP.2008.33

Nergiz ME, Atzori M, Saygin Y. (2008). Towards trajectory anonymization: A generalization based approach, //*SPRINGL '08: Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, P52–61. https://doi.org/10.1145/1503402.1503413

Nissenbaum H. (2004) Privacy as Contextual Integrity, *Washington Law Review*, Vol.79(1):119-158. https:/doi.org//10.2307/4141925

Nissenbaum H. (2009). *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, USA, P233.

NIU Xinyi, DING Liang, SONG Xiaodong. (2014). Understanding Urban Spatial Structure of Shanghai Central City Based on Mobile Phone Data, *Urban Planning Forum*, (6):61-67. http://dx.chinadoi.cn/10.3969/j.issn.1000-3363.2014.06.009

Niu Xinyi, Wang Yao, Ding Liang. (2017). Measuring Urban System Hierarchy With Cellphone Signaling, *Planners*, Vol.33(1):50-56. http://dx.chinadoi.cn/10.3969/j.issn.1006-0022.2017.01.008

PEARCE H. (2017). Big data and the reform of the European data protection framework:An overview of potential concerns associated with proposals for risk management-based approaches to the concept of personal data, *Information & Communications Technology Law*, Vol.26(3)：312-335. http://dx.chinadoi.cn/10.1080/13600834.2017.1375237

Qi Aimin, Shao Guosong, Zheng Wentong. (2018). Assessing China's Cybersecurity Law, *Computer Law &*

Security Review, Vol.34(6): 1342-1354. https://doi.org/10.1016/j.clsr.2018.08.007

QI Aimin, ZHANG Zhe. (2018). Identification and reidentification: The definition of personal information and the legislative choice, *Journal of Chongqing University(Social Science Edition)*, Vol.(2):119-131. http://dx.chinadoi.cn/10.11835/j.issn.1008-5831.2018.02.011

Raff M. (2015). The importance of reforming civil law in formerly socialist legal systems, *International Comparative Jurisprudence*, Vol.1(1):24-32. https://doi.org/10.1016/j.icj.2015.10.007

Renger R, Gotkin V, Crago M, Shisslak C. (1998). Research and legal perspectives on the implications of the Family Privacy Protection Act for research and evaluation involving minors, *The American Journal of Evaluation*, Vol.19(2):191-202. https://doi.org/10.1016/S1098-2140(99)80194-5

Rocher L, Hendrickx JM, Yves-Alexandre de Montjoye. (2019). Estimating the success of re-identifications in incomplete datasets using generative models, *Nature Communications*, Vol.10(1). https://doi.org/10.1038/s41467-019-10933-3

Shen Zhenjiang, Li Miaoyi. (2018). *Big Data Support of Urban Planning and Management:The Experience in China*, Springer, Berlin, P239-254. https://doi.org/10.1007/978-3-319-51929-6

Sinn D, Kim S, Syn SY. (2019) .Information activities within information horizons: A case for college students' personal information management, *Library & Information Science Research*, Vol.41(1):19-30. https://doi.org/10.1016/j.lisr.2019.02.003

Solove DJ. (2013). Introduction: Privacy Self-Management and the Consent Dilemma, *Harvard Law Review*, Vol.126(7):1880-1903. https://doi.org/10.2307/23415060

Steppe, R. (2017). Online price discrimination and personal data: A General Data Protection Regulation perspective, *Computer Law & Security Review*, Vol.33(6):768-785. https://doi.org/10.1016/j.clsr.2017.05.008

Sun L, Tang Y, Zuo W. (2020). Coronavirus pushes education online. *Nature Materials*, 19(6):687-687. https://doi.org/10.1038/s41563-020-0678-8

Sun Zhengwei. (2016). The Legal Mode of the Protection of Personal Information in the Age of Big Data, *Researches in Library Science*, 2016, (9):72-76,65 http://dx.chinadoi.cn/10.15941/j.cnki.issn1001-0424.2016.09.012

Svantesson DJB. (2018). Enter the quagmire – the complicated relationship between data protection law and consumer protection law, *Computer Law & Security Review*, Vol.34(1):25-36. https://doi.org/10.1016/j.clsr.2017.08.003

Tian Ye. (2018). The dilemma and outlet of informed consent principle in the era of big data:A case of personal information protection of biological database, *Law and Social Development*, Vol.24(6):111-136.

Tikkinen-Piri C, Rohunen A, Markkula J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies, *Computer Law & Security Review*, Vol.34(1): 134-153. https://doi.org/10.1016/j.clsr.2017.05.015

Tracol X. (2015). Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it, *Computer Law & Security Review*, Vol.31(1):112-119. https://doi.org/10.1016/j.clsr.2014.11.007

Unger S, Meiran W. (2020). Student attitudes towards online education during the COVID-19 viral outbreak of 2020: Distance learning in a time of social distance, *International Journal of Technology in Education and Science (IJTES)*, Vol. 4(4):256-266. https://doi.org/10.46328/ijtes.v4i4.107

Vandercruysse L, Buts C, Dooms M. (2020). A typology of Smart City services: The case of Data Protection Impact Assessment, *Cities*, Vol.104, No.102731. https://doi.org/10.1016/j.cities.2020.102731

WANG De, GU Jiahuan, YAN Longxu. (2018). Delimiting the Shanghai metropolitan area using mobile phone data, *ACTA GEOGRAPHICA SINICA*, Vol.73(10):1896-1909. http://dx.chinadoi.cn/10.11821/dlxb201810006

WANG De, ZHONG Wei jing, Xie Dong can, et al. (2015). The Application of Cell Phone Signaling Data in

the Assessment of Urban Built Environment: A Case Study of Baoshan District in Shanghai, *Urban Planning Forum*, (1): 82-90. http://dx.chinadoi.cn/10.16361/j.upf.201505010

WANG Jiayao, WU Fang, GUO Jianzhong, et al. (2017). Challenges and Opportunities of Spatio-temporal Big Data, *Science of Surveying and Mapping*, Vol.42(7):1-7. http://dx.chinadoi.cn/10.16251/j.cnki.1009-2307.2017.07.001

Wang Liming. (2019). Data Sharing and Personal Information Protection, *Modern Law Science*, Vol.41(1):45-57. http://dx.chinadoi.cn/10.3969/j.issn.1001-2397.2019.01.04

Wang Liming, (2021a). Personal Dignity: The Primary Value of the Personality Rights in the Civil Code, *Contemporary Law Review*, Vol. 35(01):3-14.

Wang Liming. (2021b). Harmonyand Difference: Demarcation and Application of Privacy and Personal Information Rules, *Law Review*, Vol. 39(02):15-24. https://doi.org/10.13415/j.cnki.fxpl.2021.02.002

Wernke M, Skvortsov P, Durr F, et al. (2014). A classification of location privacy attacks and approaches, *Personal & Ubiquitous Computing*, Vol.18(1):163-175. https://doi.org/10.1007/s00779-012-0633-z

Westin AF. (1967). *Privacy and Freedom*, The Bodley Head Ltd., London, p7.

XIANG Dingyi. (2018). On the independence of personal information property right, *Journal of Chongqing University (Social Science Edition)*, Vol. 24(6):169-180. http://dx.chinadoi.cn/10.11835/j.issn.1008-5831.2018.06.016

Xiao Y, Xiong L. (2015). Protecting locations with differential privacy under temporal correlations, //*Proceedings of ACM Sigsac Conference*, Denver, CO, USA, P1298-1309. https://doi.org/10.1145/2810103.2813640

YAN Qing, LI Cheng-gu, CHEN Cai, et al. (2018). CHARACTERISTICS OF ACTIVITY SPACE AND COMMUNITY DIFFERENTIATION IN CHANGCHUN: A STUDY USING MOBILE PHONE SIGNALING DATA, *HUMAN GEOGRAPHY*, Vol.33(6):35-43. http://10.13959/j.issn.1003-2398.2018.06.005

Yang Lang, Zhou Lina, Zhang Xiaoming. (2019). Research and evaluation of Jobs-Housing Space Characteristics based on Mobile Phone Signaling Data: A Case Study of Guangzhou, *Urban Insight*, (3): 87-96. http://dx.chinadoi.cn/10.3969/j.issn.1674-7178.2019.03.008

YANG Weiqing. (2016). Inspecting Ownership Pattern of Personal Information in Value Dimension, *Law Review*, Vol.34(4):66-75. http://dx.chinadoi.cn/10.13415/j.cnki.fxpl.2016.04.008

YIN Jian-li, WANG Zhong. (2016). System of Personal Data Traceability Management under the Big Data Environment, *Information Science*, Vol.34(2):139-143. http://dx.chinadoi.cn/10.13833/j.cnki.is.2016.02.028

Yu Xiaolan, Zhao Yun. (2019). Dualism in data protection: Balancing the right to personal data and the data property right, *Computer Law & Security Review*, Vol.35(5), No.105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yu Xin, Xie Zhi-qiang, Jing Yang. (2017). The privacy preserving method for dynamic trajectory releasing based on adaptive clustering, *Information Sciences,* Vol.378:131–143. https://doi.org/10.1016/j.ins.2016.10.038

Yuan Yihong, Raubal Martin, LiuYu. (2012). Correlating Mobile Phone Usage and Travel Behavior: A case study of Harbin, China Computers, *Environment and Urban Systems*, Vol.36(2): 118-130. https://doi.org/10.1016/j.compenvurbsys.2011.07.003

Zang Hui, Bolot J. (2011). Anonymization of Location Data does not Work: A Large-scale Measurement Study, //*MobiCom '11:Proceedings of the 17th Annual International Conference on Mobile Computing and Networking, Las Vegas, Nevada, USA*，ACM Press, New York, P145-156．https://doi.org/10.1145/2030613.2030630

ZENG Li-jie. (2007). A Contrastive Analysis of the Chinese and Western Privacy Right, *JOURNAL OF HUBEI UNIVERSITY（PHILOSOPHY AND SOCIAL SCIENCE）*, Vol.34(4):35-39. http://dx.chinadoi.cn/10.3969/j.issn.1001-4799.2007.04.013

ZHANG Jun, (2021). Personal Information Protection：Beyond the Limitation of Individual Right Thinking,

Journal of Dalian University of Technology(Social Sciences), Vol. 42(01):90-97. https://doi.org/10.19525/j.issn1008-407x.2021.01.011

ZHANG Lei, MA Chunguang, YANG Songtao, et al. (2017). Real-time similar trajectory generation algorithm for resisting trajectory difference identification attack, *Journal of Harbin Engineering University*，Vol.38(7): 1173 -1178. https://doi.org/10.11990/jheu.201605070

Zhang Tianran. (2016). Job-Housing Spatial Distribution Analysis in Shanghai Metropolitan Area Based on Cellular Signaling Data, *Urban Transport of China*, Vol.14(1): 15-23. http://dx.chinadoi.cn/10.13813/j.cn11-5141/u.2016.0103

Zhang Xinbao. (2015). From Privacy to Personal Information:The Theory of Interest Remeasurement and Institutional Arrangement, *China Legal Science*, (3):38-59. https://doi.org/10.14111/j.cnki.zgfx.2015.03.003

Zhang Yong. (2020). Legal Protection of Personal Information Related to the Epidemic in the Context of Big Data, *Henan Social Sciences*, Vol.28(4):56-65. http://dx.chinadoi.cn/10.3969/j.issn.1007-905X.2020.04.007

Zhao Bicheng, Tang Xiaoyong, Gao Zhigang, et al. (2019). *Method for user activity space identification based on mobile phone signaling*: China, 2019106291465 [P/OL]. 2019-07-12[2020-02-27].

ZHAO Pengjun, HU Haoyu, HAI Xiaodong, et al. (2019). Identifying Metropolitan Edge in City Clusters Region Using Mobile Phone Data: A Case Study of Jing-Jin-Ji, *Urban Development Studies*, Vol.26(9):69-79. http://dx.chinadoi.cn/10.3969/j.issn.1006-3862.2019.09.014

Zhong Jianyou, Chang Shan, Liu Xiaoqiang, et al. (2016). De-anonymization Attack Method for Mobile Trace Data, *Computer Engineering*, Vol.42(12) : 133-138. https://doi.org/10.3969/j.issn.1000-3428.2016.12.024

ZHONG Weijing, WANG De, XIE Dongcan, et al. (2017). Dynamic characteristics of Shanghai's population distribution using cell phone signaling data, *Geographical Research*, Vol.36(5): 972-984. http://dx.chinadoi.cn/10.11821/dlyj201705013

ZHOU Shui-Geng, LI Feng, TAO Yu-Fei, et al. (2009). Privacy Preservation in Database Applications:A Survey, *CHINESE JOURNAL OF COMPUTERS*, Vol.32(5): 847-861. http://dx.chinadoi.cn/10.3724/SP.J.1016.2009.00847

ZHOU Yi-fan, (2019). Legal Regimes for Data Protection: Digital Property or Fundamental Individual Rights, *SCIENCE·ECONOMY·SOCIETY*, Vol.37(4):93-99. https://doi.org/doi:10.3969/j.issn.1006-2815.2019.04.013