Scientific Research Publishing

Open Journal of Social Sciences, 2021, 9, 17-30
https://www.scirp.org/journal/jss
ISSN Online: 2327-5960
ISSN Print: 2327-5952

Research on Personal Data-Related Crime in China

Bingchen Chen

East China University of Political Science and Law, Shanghai, China
Email: chenbingchen@hotmail.com

How to cite this paper: Chen, B. C. (2021). Research on Personal Data-Related Crime in China. *Open Journal of Social Sciences, 9,* 17-30.
https://doi.org/10.4236/jss.2021.99002

Received: August 5, 2021
Accepted: August 29, 2021
Published: September 1, 2021

Abstract

With the development of science and technology, digital products come into our life and play an important role. China has now entered the digital society, and Surf the Internet has become a daily habit for most people. While we enjoy the convenience of life brought about by the Internet, the huge personal data leakage problem lies in front of the whole society. Citizens' personal data has rich connotations, so it needs to be classified properly. The crime of infringing on citizens' personal data is extremely harmful and requires active governance. Individual citizens, enterprises, and governments should all participate in the crime of protecting citizens' personal data.

Keywords

Personal Data, Crime, Data Safety, China Legal

1. Introduction

Since the development of Internet in China mainland from the end of twentieth century, just 20 years, the embryonic form of a digital society has been established. As you can directly perceive today: swipe your fingertips on shopping apps such as Taobao, you can easily browse a wide range of products, and get your favorite products in your hands through online payment, instead of doing the same as before. Practicing, working hard, losing yourself in the vast market; remember the scene of queuing to pay? Today, State Grid Corporation of China provides their APIs to online payment platforms such as Alipay and WeChat, and there is no need to power rate in long lines. The cellphone prepaid card has gradually become a history. As long as mobile phone connected to the Internet, you can top up anytime and anywhere; Travel is easier, we can buy train tickets and air tickets online easily, and there is no need to go to the train station or terminal station. The long queue does not go through the cumbersome booking process of air tickets. With the comprehensive deployment of 5G networks and the widespread deployment of IPv6 technology, which claims to be able to encode every grain of sand on the earth, we believe in that life can be better with the development of Digital society.

There's an old saying that "Misfortune might be a blessing in disguises" by Chinese philosopher Laozi. While we enjoy the convenience of life brought about by the Internet, the tremendous personal data leaked problems lies in front of the whole society. Especially with the implementation of the national network real-name system, related supporting systems have not kept up, making individuals extremely vulnerable to the risk of personal information data leakage. In recent years, criminal cases of infringement of citizens' personal data have occurred frequently, causing huge property losses to the people. How to manage the crime of infringing on citizens' personal data has become the content of this article.

2. Personal Data

2.1. The Difference between Personal Information and Data

In general, the concept "personal information" equal to "personal data", however, it is different. Wikipedia's data article shows that although the terms "data" and "information" are often used interchangeably, these terms have distinct meanings. Mei shows that data and information are different in nature. First the concepts of data and information are in a mixed state. Then Mei explained his view at the 2020 Data Security Law Conference of People's Public Security University of China, information is defined by content and data is the manifestation of information. All in all, information is a form of digital data, protecting information is equivalent to protecting data. Cheng shows that data is an independent object, and has property characteristics base on civil law (Cheng & Wang, 2020). Li shows a similar view that the value, controllability and independence of data make it a new type of property (Li, 2020). From the above research conclusions, we can conclude that the value attribute of the data has been wildly accepted by most researchers (An, 2021; Huang & Chen, 2021; Ren, 2021).

What is data? In China, most computer nouns are directly translated from the origin English nouns. The Wikipedia shows that Data are units of information, often numeric, that are collected through observation. Generally speaking, owing to data lack of organization and classification, it cannot clearly express the meaning of things. It may be a pile of magazines, a stack of newspapers, several meeting records, or the entire patient's medical records. Data describes the symbolic records of things, which are entities that can be defined as meanings, and involve the existence of objects. It is a set of discrete and objective factual descriptions about an event, and it is the original material that constitutes news and knowledge. Therefore, from the view of the definition of data, information is the manifestation of data. Data is a basic unit of information. Therefore, if data is leaked, it is more harmful than leaking information.

2.2. The Content of Personal Data

2.2.1. General Data Protection Regulation

General Data Protection Regulation, or GDPR, is currently implemented uniformly in 28 EU member states. Although the effectiveness of the EU GPDR is basically limited to the EU, it still does not affect it as a law that shocks the world. After the GPDR was promulgated, Google and Facebook became the main targets due to their high compliance requirements (Sheng & Yang, 2020).

The first item of Article 4 of the GPDR defines personal data. "Personal data" refers to any information related to an identified or identifiable natural person ("data subject"); an identifiable natural person refers to a person who can be directly or indirectly identified, especially by reference such as name, identification number, location Data, identifiers such as online identifiers, or specific to the physical, physiological, genetic, psychological, economic, cultural, or social identity of the natural person.

GDPR takes personally identifiable information as its core concept. All relevant information that can be used to identify individuals falls within the scope of GDPR protection. This information is no longer just a name, phone number or address, but also includes browser cookies, IP location, or biometrics and medical information sufficient to identify a person. The specific classification includes the following:

1) Basic identity information

Basic identity information is the information most commonly used by each person in society, such as real name, household registration address or residential address, ID card number, etc. Basic identity information can quickly determine whether a person is himself, so the risk of leakage is also the greatest.

2) Personal network data

Common ones are geographic location, IP address, Cookie's data and RFID tags. Because mobile devices generally have WIFI, Bluetooth and other functions, even if you don't need a GPS sensor, you can judge where you are through your network environment. The disadvantage is that the accuracy is not enough. Regarding the IP address, it is different from China and overseas due to IPv4 technology. Be the first to apply, and the number of address pools is sufficient. Both companies and individuals can achieve fixed IP access (due to the late start of the Internet in Mainland China, there are not many IPv4 addresses left in the world, and most of them use shared IP to surf the Internet); Cookie's data refers to the storage in the data on the user's local terminal, the invention of this technology is mainly for the website to identify the user's identity. For example, when you completely close the browser and open the website you have just logged in, it will automatically log in without having to re-enter the account password; RFID tag, that is, electronic tag system. The most used in daily life is to swipe the meal card. However, with the establishment of the Internet of Things, smart homes have moved towards millions of households. Smart homes usually use this technology to identify users' wireless operations.

3) Medical care and genetic data

Medical care data refers to personal data related to the physical or mental health of a natural person, including data provided by health care services that can reveal his or her health. Genetic data refers to data that reflects the law of personal inheritance.

4) Biometric data

Refers to data that determines identity by identifying biological data, such as fingerprints and face data. There are also racial or ethnic data, political opinions, and sexual orientation.

2.2.2. China "Information Security Technology—Personal Information Security Specification"

On May 1, 2018, the "Information security technology—Personal information security specification" was formally implemented. This specification is called the "GPDR Chinese version" in the industry. Indeed, the regulations were formulated with reference to the most advanced foreign legislation in the protection of personal information, such as GDPR (General Data Protection Regulation), EU-US Privacy Shield (European and American Privacy Shield Agreement), Consumer Privacy Bill of Rights (US "Consumer Privacy Rights Act"). It should be noted that this specification is not a mandatory specification but implemented as a national recommended standard. However, it will be a reference standard for my country to carry out various activities related to personal information protection in the future, and it will also become the development and implementation of personal information protection in the future. The basis of relevant laws and regulations

The specification not only defines personal information, but also provides a logic for determining whether it is personal information. The specification defines personal information as a variety of information recorded electronically or in other ways that can identify a specific natural person alone or in combination with other information or reflect the activities of a specific natural person. To determine whether a piece of information belongs to personal information, the following two paths should be considered: one is identification, that is, from information to individual, specific natural persons are identified by the particularity of the information itself, and personal information should help identify specific individuals. The second is association, that is, from individual to information. If a specific natural person is known, the information generated by the specific natural person in its activities (such as personal location information, personal call records, personal browsing records, etc.) is personal information. Information that meets one of the above two situations shall be judged as personal information.

Compared with GDPR, although there are overlapping classifications, the classifications are obviously richer. It specifically includes basic personal information, personal identification information, personal biometric information, network identification information, personal health and physiological information, personal education and work information, personal property information, personal communication information, contact information, personal Internet records, and personal common device information, Personal location information and other information. Compared with the GDPR, the standard information is classified into basic personal information, personal property information, personal communication information, and personal digital devices information.

Basic personal information refers to data that records personal background characteristics. Personal name, birthday, gender, ethnicity, nationality, family relationship, address, personal phone number, e-mail address, etc.

Personal property information refers to data that can reflect personal property. For example, bank account number, identification information (password), deposit information (including the amount of funds, payment and collection records, etc.), real estate information, credit records, credit information, transaction and consumption records, flow records, etc., as well as virtual currency, virtual transactions, Virtual property information such as game redemption codes.

Personal communication information refers to data that can record personal communication through media. For example, communication records and content, SMS, MMS, e-mail, and data describing personal communications (usually called metadata), etc.

Personal digital devices information refers to the hardware data with networking functions used by oneself. Refers to information describing the basic situation of personal commonly used devices, including hardware serial number, device MAC address, software list, unique device identification code (such as IMEI/android ID/IDFA/OPENUDID/GUID, SIM card IMSI information, etc.).

2.3. The Proper Classification of Personal Data

Both the EU GDPR and my country's "Personal Information Security Regulations" have made relatively complete definitions and types of personal information data, both of which emphasize the personal identifiability of data information (Wang & Wang, 2021). The difference is that the EU emphasizes the identity of a "digital subject", while my country emphasizes the identity of a "natural person". The EU does not impose definitional restrictions on the form of data existence, and my country clearly proposes "recorded by electronic or other means." However, the most fundamental difference is that the term adopted by the EU is "data", while the term adopted by my country's specification is "information." At the same time, the division of data is too broad, which will put greater pressure on corporate compliance and is not conducive to innovation; if the scope of the division is too narrow, it will not play a role in protecting personal data.

Therefore, based on the results of the above analysis of data and information, the personal data can be summarized into the following categories:

Personal basic data. Basic personal data refers to data that can quickly identify and locate the person and has a basic role in identifying an individual. The specific connotation is name and ID data.

Personal data. Refers to the data that can complete the description of the personal life track. Specific connotations should include residential address, work address, activity location, shopping location, school location, and smart home data. After obtaining personal daily life data and performing coding rearrangement, you can fully understand the individual's daily routine habits and various preferences. Although it is currently mostly used for advertising, once it is acquired by criminals, the individual will enter a state of being "not afraid of thieves, but afraid of thieves".

Personal social data. Social interaction is an indispensable behavior for human beings, and it is also a skill that people in society must possess. Therefore, social data refers to data that can record and reflect a person's social situation. Specifically, it includes data such as phone numbers and call records, social accounts, emails, instant messages, and BBS.

Personal property data. Refers to data that can reflect personal property. Specifically, it should include bank account numbers, authentication information (passwords), deposit information (including the amount of funds, payment and collection records, etc.), real estate information, credit records, credit information, transaction and consumption records, and flow records. The author has reservations about the virtual property information included in the personal property data in the "Personal Information Security Regulations", because virtual property information is generated after personal property is consumed and should be a commodity. It can only reflect how much a person spends Money; it is impossible to judge how much money he has. For example, if a child charged tens of thousands of yuan to his game account, it does not reflect the child's own situation. Therefore, virtual property information does not meet the criteria for data originality.

Personal device data. Personal device data should be device data that can be connected to the Internet. Just like the types of device data listed in the "Personal Information Security Specification", the hardware serial number, device MAC address, and unique device identification code can identify individual devices through these data. If these devices are not connected to the Internet, in fact, the leakage of device data will not do any harm to individuals. For example, a traditional washing machine is placed in the home, and only the master can manipulate it. However, if this washing machine is connected to the Internet and can be individually identified and determined on the network, then it is not only the owner who can manipulate the washing machine. Therefore, personal device data should refer to the data of those personal networked devices. For example, current mobile phone devices are equipped with GPS chips. After obtaining the information of the mobile phone device, the individual's whereabouts can be read.

3. Harmfulness of Crimes against Citizens' Personal Data

The famous case "Xu" to make society of China mainland realized the important of personal data. Xu, a college-bound student, died after suffering a sudden cardiac arrest on Sunday after funds her family had raised for her tuition fees were swindled in a telephone scam. Xu's tuition was defrauded by offends, for the reason that the offender through phone to tell her real data to be trusted. The harm of the crime of infringing on citizens' personal data lies in exposing each "digital" individual "naked" to the society.

3.1. The Harm of Personal Basic Data Leakage

At present, ID is the passport for life services in Mainland, and it has the most extensive application scenarios. Nowadays, you can use digital ticket, after you buy ticket online and the digital ticket data will link your ID cards automatically, then you can use Id alternatively in and out of the station. The hotel, financial industry, logistics, and transportation industry have all been connected to the ID card authentication system. The ID is the most commonly used personal data, and easily illegal used by various subjects. The final result is that the ID number has become the first data leaked.

On September 6, 2020, according to Nandu Daily, a female fan of Wu, Lei (the actor of the Fei Liu of TV series "Langya Bang") stole his earn miles of China Southern Airlines to redeem free air tickets for herself and her friends from 2017 to 2020, up to 12 times. According to an informant, the way of this woman to do this thing is to bound Wu Lei's ID to the airline account she registered with her mobile phone number. Through this operation, this fan can not only view Wu Lei's travel schedule anytime, but can also add beneficiary link to this account without Wu, lei's authorization. Therefore, the leakage of personal data can give others the opportunity to do Identity theft.

In addition, the ID generate rules are transparent to the society. By analyzing the ID number, you can obtain valid information such as your place of birth, time of birth, and gender.

3.2. The Harm of Personal Activities Data Leakage

In the past, personal activities were private, and it was hard for others to know where they were, what they bought, and the road map. Even if they used public power to draw a diagram of a person's activities still need a lot of resources to support. Nowadays, due to the popularization of smart phones and everyone take along smart phones in daily life at any time, the collection of personal activities data has become easier. However, the mobile phone operating system has relatively loose authority management for APP, the APP installed on the user's mobile phone can collect the user's daily activities data and exchange it between different enterprises without the user's authorization.

On April 13, 2018, Chinese netizen @Eric Tsui posted a set of pictures on Weibo, showing that two people use Didi app (taxi software) to start from the same place and the same destination, but charge different prices. According to Beijing Daily, whether industrial age or information age, segment market is a kind of trend, for the reason that enterprises need to get higher marginal benefits. Marginal benefit refers to the additional benefit arising from a unit increase in a particular activity. The general operation is to set a high price for those with high demand, and set a low price for those who would not buy if the price is high. In the era of industrial age, enterprises need to invest a lot of resources to conduct market research to segment the market. However, in the information age, enterprises can only use special APP or purchase relevant data from data enterprises to achieve their goals.

If your activities data is leaked, it will be able to make a portrait of your life habits after being used by the relevant subject. For enterprises, they can recommend products to you at your expected price at a precise time and point to encourage you to consume, or they can use big data technology to discriminate customers. The offends can carry out criminal activities during your rest time according to your living time, such as send fake messages through fake mobile communication base station.

3.3. The Harm of Personal Social Data Leakage

The main hazard of personal social data leakage is to make one's own social relations public.

Recoding and analysis of personal social data can effectively obtain a personal network. The most common behavior is to read the address book by the APP in the smartphone. When you are using Tik Tok, you will be pushed to "people you may know". After the Tik Tok APP reads the phone address book, it not only recommends the people in the address book, but also recommends the second-level relationship of the people in the address book, which is generally displayed as "common contact". The recommendation mechanism of Tik Tok reflects the power of the Tik Tok algorithm. Although it brings great portability for users' social interaction, it also violates users' privacy. Some netizens said that I just want my Tik Tok to be my "back garden" and I don't want to share it with others.

WeChat has now become a Chinese national social app, and the number of downloads ranks first in all app stores. However, do you know that strangers request to add WeChat friends to hide their routines? Due to the certain features of WeChat, users are recommended to enable "Discover Friends in the Address Book" function to obtain the permission to read the phone's "Address Book". When you add a new phone number to your mobile phone address book, WeChat will automatically recommend that the people linked to this number to you. Offenders use this function to perform reverse operations, buy active mobile phone numbers, import their own mobile phone address book, and then add friends through the "discover friends in address book" function of WeChat. According to news reports, after a stranger has successfully added a friend, he usually recommends financial products or sells tea, but the ultimate goal is to defraud the victim's money. Therefore, after personal social data is leaked, criminals can be provided with opportunities to contact victims.

Another common crime is to use the conditions of asymmetry in the time information of social relationships to defraud relatives and friends. In recent years, the most common case of "virtual kidnapping of overseas students" is that scammers pretend to be the Chinese embassy in the UK or the International Criminal Police Organization, and use technical means to call Chinese students in the UK by fraudulently using the phone numbers of relevant agencies to call Chinese students in the UK. The parties or their parents are suspected of serious crimes. If they do not cooperate with the "investigation", they will be wanted or arrested, and they will be controlled and guided to take pictures or videos of themselves being tied up, beaten, and crying to their parents for rescue for reasons such as "necessary to handle the case." Subsequently, he used the obtained audio-visual materials to defraud parents far away in China for a huge ransom.

There are also cases of using social accounts to defraud friends. The specific operation is to purchase a decrypted QQ number online and log in, impersonate the QQ to contact a friend, swindling money on the grounds that the parents and friends are sick and need medical treatment.

3.4. The Harm of Personal Property Data Leakage

Due to the continuous evolution of security strategies in the financial industry in recent years, the current payment adopts multiple verification security strategies, such as dual verification of mobile phone verification codes, so the leakage of bank account passwords alone generally does not pose a threat to personal property. Under the above background, theft still occurs, most of the criminals use the leaked personal data and adopt social work strategies to make the victim to provide all the information in order to achieve the criminal purpose.

However, such as deposit information, real estate information, credit records, credit information, transaction and consumption records, flow records, etc., if the data that everyone cares about the most is leaked, it will have a greater threat to itself. For example, in the credit business, in order to prevent and control lending risks, both regulatory authorities and banks have made strict regulations on the process and review of lending business. Among these requirements, the first priority is to verify the identity of the applicant. The applicant must provide a series of information including ID card, income certificate, loan purpose, etc., and the bank must verify that it meets the requirements. According to relevant media reports, the criminals successfully obtained the loan by replacing the original owner's photo on the ID card and relying on the original owner's property records.

3.5. Harmfulness of Personal Network Devices Data Leakage

In the Hollywood sci-fi blockbuster "Terminator" and "Resident Evil", everyone has already experienced the scene of robot chasing and killing humans in advance. The only way for the protagonists of the two movies to avoid being chased by machines is to hide as much as possible in places without internet access. Although this scene is still far away from us, each of us currently owns more and more networked devices, and the problem of privacy leakage also comes with it.

At the end of 2017, the 360 smart Video camera live broadcast event broke out. The biggest selling point claimed by the 360 smart Video camera is that by connecting to the Internet, users can view real-time images in the home or monitored scene through the smart camera anytime and anywhere. But then it broke out that 360 privately broadcast the user monitoring screen to the public without the user's permission. At the same time, there are many private life videos with 360 watermarks on the Internet. 360 company is a network security company, why does such a thing happen? According to "China Business News", there is a transaction on the market to sell related cracked software, surveillance video, and camera ID and password. The unit price of a surveillance camera ID and password can be obtained at a minimum of 4 yuan, and the unit price of a private video is only One yuan is required. Li, Tiejun, a security expert at Cheetah Mobile, revealed to the media: "In fact, the vulnerabilities of the surveillance digital devices have long been made public. Due to the negligence of traditional manufacturers, hardware vendors should take the main responsibility in it."

Data leakage of personal networked devices mainly refers to the leakage of Mac address, bound IP address, port, and device authentication password data. Through the above data, with the help of the Internet, people with unruly motives can arbitrarily control personal networked devices in the background to achieve illegal purposes.

4. The Strategies about Protect Personal Data

As mentioned, the numerous and serious harms caused by the infringement of personal data are urgent. According to the special action "2020 Net Network" of Ministry of State Security of the PRC', a total of 57 illegal text messaging platforms that provide services for loan-type telecommunications network fraud criminal gangs have been destroyed, and 798 suspects have been arrested. During the COVID-19 pandemic, the national public security and Internet security departments cracked down on online criminal activities that violated citizens' personal information (Wei & Zhang, 2021). They have punished 1522 people and notified other departments to impose party disciplinary and political sanctions on 433 people. However, special actions by the Ministry of Public Security are far from enough. Preventing the infringement of citizens' personal data requires the cooperative efforts of individuals, enterprises, and governments, as well as the governance of multiple links such as prevention, monitoring, and prevention (Ding, 2021).

4.1. Individual Citizens Should Care Their Personal Data

It is common for individual citizens to have a weak awareness of the protection of their personal data (R. Wang, 2021). For convenience, most people store ID photos and other ID photos in their mobile phones without encryption protection. Once the mobile phone is lost, criminals can use the data in the mobile phone to quickly make a manual appeal, obtain the ownership of the relevant account, and conduct illegal operations. In the study and work, it is often necessary to report the ID card and other data. After the declaration is completed, the local terminal will not delete the data, which may lead to the possibility of others having the opportunity to learn their personal information (Li, 2021). The most dangerous operation is that most people store their ID cards at will, making the ID cards accessible to more people. In addition, there are also the well-known express delivery slips, most of which show the recipient's address, number and name on the face. Many people do not erase the information on the express delivery slips after receiving the express, so an industry that specializes in collecting data on the face sheets of abandoned express boxes (L. Wang, 2021).

Individual citizens should protect their account passwords. You should manage your own account by yourself, and do not authorize or share account passwords to others unless necessary. In recent years, the college entrance examination tampering with volunteers has happened frequently. For example, in the case of Jiao Zhou, Shandong candidates tampering with the candidates' volunteers, the tamperer Guo and the tampered person Chang Sheng used the same computer to fill in the college entrance examination volunteers. When Chang Sheng reported, Guo stole it, Changsheng's password. The motive for committing the crime was that both of them applied for free normal students in the same major of Shaanxi Normal University, and Guo had a score lower than Chang Sheng, so he modified Chang Sheng's willingness to increase his chances of admission. In addition, many cases of tampering with college entrance examination candidates in Shanxi Pingyao, Zunyi college entrance examination candidates in Guizhou, and Qingdao college entrance examination candidates were all caused by individuals failing to protect their account passwords or revealing their account passwords to others.

Individual citizens should strictly manage APP permissions on their smart devices (Sun & Wang, 2021). At present, the two major mobile device operating systems in the world are the Android system of Google Inc. and the iOS system of Apple Inc., both of which can implement powerful APP permission management functions. Different from the closed source feature of the iOS system, the Android system can run on a variety of different hardware platforms due to its open source, and currently accounts for more than 70% of the global share. Due to the openness of the Android platform, the problem of excessive permissions for apps running on the platform has always been serious. When granting APP permissions, individual citizens should adhere to the principle of least permission granted, so as to avoid the risk of their personal data being infringed.

4.2. Enterprises Should Comply Their Obligations to Protect Consumer Data

No matter how personal citizens protect their data from being leaked, for their own convenience in online life, they will still provide their personal data to the company for storage in order to accept the services provided by the company. As the main individuals in market economic activities, enterprises should actively protect relevant data in accordance with the law. At the same time, as a trusted party in the transaction, it should actively perform its obligations.

Enterprises have the obligation to strictly prevent the leakage of user account data. On March 19, 2020, a user discovered that 538 million Weibo user information was sold on the dark web, of which 172 million had basic account information related to user ID, gender, geographic location, etc. Then Weibo quickly admitted that the Weibo data leak was true. In addition, the express delivery industry is also very weak in protecting customer information. At present, the express delivery industry mainly focuses on the speed of delivery and does not pay attention to the security of customer data.

Enterprises are obliged to prohibit the purchase and exchange of user data. On September 12, 2020, at the Global Entrepreneurs Summit, Kai-Fu Lee shared his experience in investing in "Megvii.inc", saying: "We helped them (Megvii.inc) in the early stage to find partners, including Meitu.inc, Ant Financial, and They got a lot of face data". The user's authorization to the enterprise is by default one-time or only granted to the enterprise to buy and sell user data with other companies. On the one hand, it violates the spirit of contract law, and on the other hand, it may expose users to greater risks of privacy leakage. A snowflake is innocent.

4.3. The Government Should Imply Its Obligation to Supervise the Market

In Analects, it shows that Inequality rather than want is the cause of trouble. In the digital society, rare market subjects discriminate against science and technology in order to get best profit. Therefore, government's Macro-economic Control is significant.

Under The core values of Chinese socialism, Government departments should actively use administrative regulations to control market behavior (Liu & Yang, 2021). This year, the Ministry of Culture and Tourism issued the "Interim Regulations on the Management of Online Tourism Operation and Services", which was officially issued on October 1, stating clearly that don't use big data technology discriminates against different customers. The "Information Security Technology Personal Information Security Specification" formulated by National Information Security Standardization Technical Committee requires that personal information should not be forced to be collected, and users should have the right to refuse personalized push. These administrative regulations provide a legal basis for users to protect their legitimate rights and interests, and actively regulate gray areas in market transactions. However, user data is rich in content, and more administrative regulations are needed to protect users' personal data in the future.

Government departments should monitor the storage location of Personal data. At present, it is not only Chinese enterprises provided digital services in mainland China, but also includes a large number of overseas enterprises. If the personal data of domestic citizens held by these overseas enterprises are transferred abroad, it may further cause the overseas leakage of citizens' personal data. At present, Apple Inc. has transferred the iCloud data of China mainland customers to “Guizhou-cloud big data” in Guizhou, China. What’s more, Microsoft and Amazon also have established a datacenter for storing China mainland customers data. With the further development of China’s reform and opening up, more and more overseas enterprises are urged to China for extending their business in the future. Therefore, it is vital to monitor data storage.

5. Conclusion

Based on comparative studies between domestic and international, this article subdivides personal data according to certain rules, and believes that the connotation of personal data should include personal basic data, personal daily life data, personal social data, personal property data, and personal networked device data. The harm of personal data leakage is huge and diverse, and crimes of infringing on citizens’ personal data request a good solution (Zheng & Li).

To control the crime of infringing on citizens’ personal data, this article starts from the three main subjects of citizens, enterprises and the government, and puts forward various useful countermeasures and opinions. However, this article does not give suggestions from the legislative level. The main reason is that legislation is a huge task, and the information of the digital society is changing. If legislation changes day and night, it will seriously undermine the stability of the law. Administrative regulations do not have this problem, they are more flexible and have compulsory force. In addition, the academic circles have not yet reached a conclusion about the definition of data, and the relevant research is not yet complete. Looking forward to the future, we will be able to see innovative measures to regulate crimes against citizens’ personal data at the legislative level.

Acknowledgements

Avoid the stilted expression, “One of us (R. B. G.) thanks...” Instead, try “R. B. G. thanks”. Do NOT put sponsor acknowledgements in the unnumbered footnote on the first page, but at here.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

An, K. (2021). The Legal Protection Mode of Personal Data Security—From the Perspective of Data Ownership. *Legal Forum, 36,* 58-65.

Cheng, J., & Wang, K. (2020). Re-Exploration of Legal Attribute of Data: Comment on Article 127 of the Civil Code. *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 32,* 67-74.

Ding, F. (2021). Selection of Personal Data Governance Models: Individual, Nation or Collective. *Journal of Huazhong University of Science and Technology (Social Science Edition), 35,* 64-76.

Huang, X., & Chen, J. (2021). Duality of Data Legal Protection—Based on the Balance of Personal Data and Data Products. *Journal of Xihua University (Philosophy & Social Sciences), 40,* 70-76.

Li, H. (2020). The Legal Attribute and Open Way of Government Data in China. *Administrative Law Review, No. 6,* 144-160.

Li, Z. (2021). Research on the Protection of Personal Data Rights in the Digital Economy Environment. *Journal of Zhaoqing University, 42,* 43-48.

Liu, C., & Yang, L. (2021). A Review of the Studies on Cultivating and Practising Socialist Core Value since the 19th National Congress of the CPC. *Journal of China Executive Leadership Academy Jinggangshan, No. 4,* 125-133.

Ren, D. (2021). The Property Interests System on Personal Data in the Light of Civil Code. *Legal Forum, 36,* 89-98.

Sheng, X., & Yang, S. (2020). Analysis on the Applicabilities and Functions of GDPR to Personal Data Protection in Open Sharing of Scientific Data. *Library and Information Service, 64,* 48-57.

Sun, D., & Wang, W. (2021). Research on the Legal Conflict and Settlement Mechanism of Cross-Border Protection of Personal Data. *Journal of Jiangsu Ocean University (Humanities & Social Sciences Edition), 19,* 50-62.

Wang, L. (2021). Conflict of Interest in the Commercial Use of Personal Data and Its Resolution. *Science of Law (Journal of Northwest University of Political Science and Law), No. 5,* 1-12.

Wang, R. (2021). Explore Chinese Legal Solutions for Personal Data Protection. *Information Security and Communications Privacy, No. 2,* 10-14.

Wang, T., & Wang, J. (2021). Definition and Classification of Personal Data Processing Actors Based on the Enlightenment of EU Paradigm to China's Legislation. *Journal of Weinan Normal University, 36,* 77-86.

Wei, J., & Zhang, D. (2021). The Value of Personal Data and the Legal Regulation of Its Use in the Governance of Online Rumors about the Epidemic. *Journal of Zhejiang University of Technology (Social Sciences), 20,* 104-110.

Zheng, F., & Li, S. (2021). The Evolution and Competition of Rights in the Era of Big Data: from Privacy Right, Personal Information Right to Personal Data Right. *Journal of Shanghai University of Political Science and Law (The Rule of Law Forum),* 1-16. https://doi.org/10.19916/j.cnki.cn31-2011/d.20210721.014