

Research Article

A Protection Model of Citizen Personal Information Administrative Law Based on BD Analysis and Edge Computing

Fang Yang 

University of Electronic Science and Technology of China, Zhongshan Institute, Zhongshan, Guangdong 528400, China

Correspondence should be addressed to Fang Yang; fangyang@zsc.edu.cn

Received 15 January 2022; Revised 12 February 2022; Accepted 14 February 2022; Published 8 March 2022

Academic Editor: Xin Ning

Copyright © 2022 Fang Yang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the continued advancement and popularization of the Internet and Edge Computing, the right to privacy of big data has taken on new meanings, and the tools available to protect citizens' personal information under administrative law have grown in number. In the context of big data, infringers frequently use the Internet as a natural barrier and medium, making it difficult to collect evidence once personal information has been leaked. This paper investigates the administrative law protection of citizens' personal information using big data analysis. In comparison to traditional society, information technology innovation has created massive information storage equipment, efficient information processing equipment, and rapid information dissemination means for human beings to protect their legitimate rights and interests. Sharing goes far beyond traditional societal competition. The study of administrative law protection of citizens' personal information in the big data era has the potential to not only advance the study of administrative law protection of citizens' personal information but also to reveal the characteristics of administrative law protection of citizens' personal information in the big data era.

1. Introduction

With the increasing development and updating of current science and technology, data information has spread all over every corner of our life. It records and carries the track of our daily life, study, and work in various forms. The administrative law that protects citizens' personal information has had a long history of development. Traditional citizens' personal information focuses solely on the tranquility of citizens' personal lives, and the purpose of maintaining citizens' personal information is to safeguard citizens' personal freedom, dignity, and happiness [1]. With the advancement and popularization of the Internet, the right to privacy in the BD has taken on new meanings, and the administrative law tools for protecting citizens' personal information have grown in number. Based on their highly developed information levels, developed countries were confronted with the problem of information security before China, and they have accumulated a wealth of experience and lessons in the process of theoretical and practical operation, which has great reference and reference significance for China to carry out

the protection of personal information rights [2, 3]. In China, privacy protection is relatively weak, and the scope of regulation is primarily focused on profit-making entities and non-governmental organizations violating citizens' personal information. In the field of public law, however, the criminal law imposes stricter requirements. When general breaches of personal information do not meet criminal standards, they are not punishable by law [4]. The social phenomena of the administrative law protection of citizens' personal information emerge one after another, which makes people uneasy. The wanton disclosure of personal information data greatly reduces the trust between people. However, China's existing privacy laws and regulations and industry self-discipline regulations have not formed a complete system, which is not enough to prevent and remedy privacy infringement. It is more rigorous to strengthen the protection of personal information from the administrative law level. Administrative law can clearly and specifically stipulate the right to request correction and relief of personal information, and the scope of regulation is more targeted [5, 6]. The concept of BD was first put forward in the 1990s, then swept like a tsunami, and was

widely known in recent years. Now, it has quickly become the theme of the times and is known as the “gold” of the 21st century [7].

In the era of BD [8], the legal protection of personal information has become an important issue facing all countries. In front of “BD” technology, we are no longer individuals with distinct personality, but a single “data” with economic value and social role [9]. The application and development of information technology represented by “Internet plus” have made data become the “oil” in the new era. Therefore, the application and development of “BD” technology have become an important opportunity and path of China’s “data power” [10]. Massive data analysis has mined and reorganized the personal information of thousands of information subjects, exposing the privacy that was intended to be concealed to the sun. In the era of BD, personal administrative law supervision is absent and management is weak. The applicable subject of administrative law is China’s administrative organ, and administrative supervision and management are its main responsibilities [11, 12]. In both the Internet era and the BD era, China’s administrative organs have been in the absence of supervision. The management of new Internet behaviors has been weak and has been unable to comply with the requirements of the times in time [13].

In the context of BD, infringers frequently use the Internet as a natural barrier and medium, making evidence collection difficult once personal information is exposed. Second, with massive data leakage, once personal information is stolen, it is integrated into the massive data, making it difficult to track down the source of the data leakage. Another major problem of rights relief is how to list the clear defendants in the litigation process [14]. The research on the protection of citizens’ personal information by administrative law in the BD era can not only deepen the research on the protection of citizens’ personal information by administrative law but also reveal the characteristics of the protection of citizens’ personal information by administrative law in the BD era, as well as provide specific reference opinions for the drafting of relevant Civil Code provisions. In comparison to traditional societies, information technology innovation has created massive information storage devices, efficient information processing devices, and quick means of information dissemination for human beings, and the collection, preservation, utilization, and sharing of personal information are far from traditional societies [15].

2. Related Work

According to reference [16], the United States has been at the forefront of personal data protection legislation. The EU’s new general data protection regulations went into effect in May 2018, adding to the vitality of the EU’s information protection legal system and providing a strong institutional guarantee for the EU’s overall data security. The old law was completely replaced by its role and scope of protection. The BD analysis method [17] is described in the literature “In Chinese legal circles, the terms “personal data” and “privacy” are frequently interchanged. There is no difference in

rank between these concepts in terms of their connotation and extension.” Personal information and privacy are frequently used interchangeably in domestic administrative law circles, and they are treated as one in their protection value hierarchy. The protection of personal information has previously been studied in other countries, as evidenced by reference [18]. In 1968, the United Nations proposed and emphasized the legal concept of “personal information protection.” In 1970, Germany passed a law protecting personal information, and three years later, Sweden, another European country, passed a similar law. According to [19], the selection of regulatory agencies should be based on fully absorbing foreign experience, safeguarding civil rights, and encouraging the network’s healthy development. The introduction of the industry self-discipline organization model into American legislation can improve the effect of social management after a thorough investigation of the national conditions. Reference [20] adopts the BD analysis method, “congenital differences such as historical conditions and different practice and development tracks of subsequent nature make legislators in different countries have different interpretations of the same concept or legal relationship, but in fact, there is little difference in its essence, and it is often adopted and applied to each other in many cases.” Reference [21] research shows that in German personal information law, the right basis of information subject is the right of information self-determination, and the premise of formulating all administrative legal norms is to ensure that citizens’ right of information self-determination is not infringed. Based on this strict awareness of right protection, most provisions in German administrative law aim to regulate the power of administrative subjects. There is a lack of a unified legal system specifically regulating personal information protection, and the laws of relevant departments are uncoordinated and conflict with one another [22]. Using BD analysis, the innovation of information technology has created a large number of information storage devices, efficient information processing devices, and fast means of information dissemination for human beings, and the collection, preservation, utilization, and sharing of personal information are far from being comparable to those of the traditional society. Reference [23] research shows that the only way to avoid unnecessary harm to people’s personal and property and other aspects is to strengthen administrative legislation and protect people’s right to privacy through law, i.e., the state’s coercive power. Chinese law only protects personal information as a right to privacy, according to reference [24]. In fact, the scope of personal data is much broader, and the administrative aspect is also a significant component. Personal information is protected in China primarily through administrative and criminal means, which provide only limited and indirect protection, as well as a lack of legal compensation and protection mechanisms.

This paper uses the BD platform to collect users’ consumption habits, income level, service dependence, and other data information, in order to give different users differential pricing, resulting in users’ property loss, based on BD analysis. People’s personal data is “peeped” in the age of big data. Being “stolen” is a possibility. People have a certain

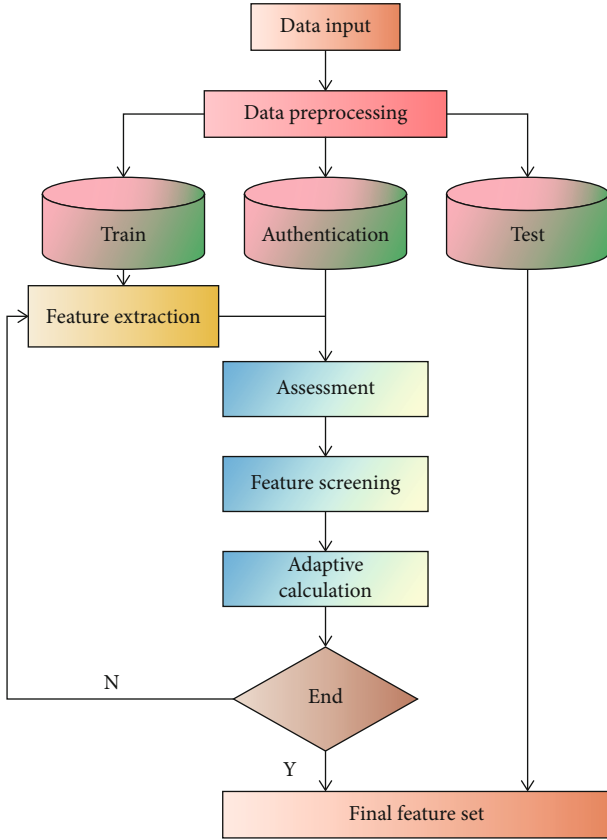


FIGURE 1: BD process description.

level of passivity when it comes to whether or not data should be used in order to avoid this risk. People's physical appearance and mental outlook are "exposed," and they have no freedom rights at the moment when "human flesh search" is popular. At present, we urgently need to establish a perfect privacy protection system to reduce the risk of BD to our privacy, solve the damage caused by the risk, and find a quiet place for our privacy.

3. Algorithm and Principle of BD

Based on their highly developed information level, developed countries were confronted with the problem of information security before China, and they have accumulated a wealth of experience and lessons in the process of theoretical and practical operation, which has great reference and reference significance for China in carrying out the protection of personal information rights. McKinsey, a well-known management consulting firm, coined the term "BD" in a 2011 research report. Data has become a key production factor in a variety of industries and functional fields. People now use ID cards to handle phone cards in the era of new networks and BD, and phone numbers are no longer just a string of numbers, but are linked to personal identity. To begin with, it should be noted that not all citizens' personal information is protected under Chinese legislation. In China, privacy protection is relatively weak, and the scope of regulation is primarily focused on profit-making entities and

nongovernmental organizations violating citizens' personal information. This demonstrates this algorithm's superior performance in achieving BD and increasing data accuracy. The description of BD process is shown in Figure 1.

The BD algorithm is designed in combination with the flow chart. The outlier similarity nodes $G_1 = (M_1^\alpha, M_1^\beta, Y_1)$ and a_{n_i} ($i = 1, 2, \dots, m$) of the BDbase are set, and the data set of feature sampling obeys t

$$\begin{cases} \dot{m}_i(t) = -a_i m_i(t) + b_i(p_i(t - \sigma), p_n(t - \sigma)), \\ \dot{p}_i(t) = -c_i p_i(t) + d_i m_i(t - \tau). \end{cases} \quad (1)$$

Set $X = (x_1, X_2 \dots \dots X_d)$ as a feature vector in the BD clustering space, use the rough concept lattice method to construct the second-order cone programming model for the BD information flow in the BDbase system, use the linear frequency modulation signal model method to fit the BD information flow by partition, and select the following decision function

$$l_2 = \max_b \left| \int r(t) \frac{1}{\sqrt{a'}} f^* \left(\frac{t-b}{a'} \right) dt \right| = \max_b \left| W_f r(a', b) \right| \begin{matrix} > \\ < \end{matrix} \begin{matrix} H_1 \\ H_0 \end{matrix} \lambda_2, \quad (2)$$

where $[A_j, B_j]$ represents the minimum and maximum values, initializes the data clustering center $f(X_i, A_j(L))$, processes the information of the data sample set by using the second-order cone programming model, and obtains the data fusion space matrix of the i th node as

$$s(t) = \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} a_{mn} g_{mn}(t), \quad (3)$$

where a_{mn} is called the convex optimal expansion coefficient of second-order cone programming, and the clustering granularity is

$$g_{mn}(t) = g(t - mT) e^{j2\pi(nF)t} m, n = 0, \pm 1, \pm 2, \dots \quad (4)$$

Calculate the weighting vectors of input nodes and output nodes in the data clustering center ω . The Euclidean distance of J , expressed as

$$d_j = \sum_{i=0}^{k-1} (x_i(t) - \omega_{ij}(t))^2, j = 0, 1, \dots, N-1, \quad (5)$$

among $\omega_j = (\omega_{0j}, \omega_{1j}, \dots, \omega_{k-1j})T$. In the data process, information scheduling is carried out in the special relationship information of useful information and knowledge, and the attribute set of feature sequence training set of BD is constructed to provide data basis for data.

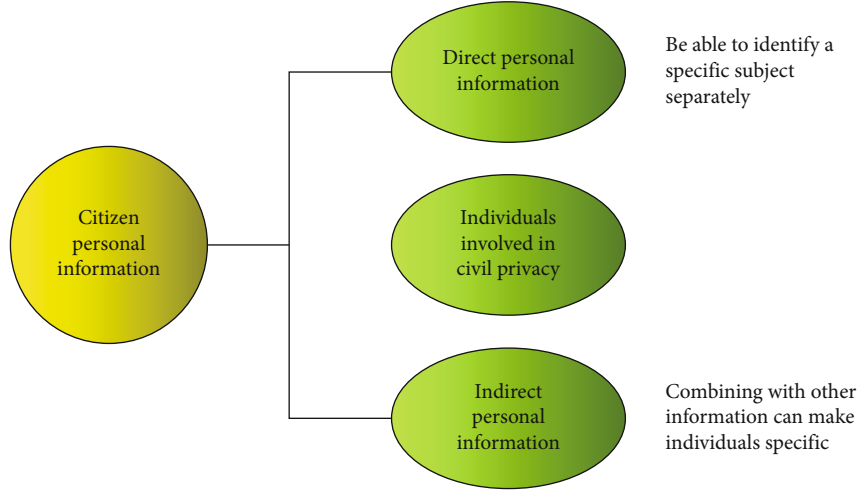


FIGURE 2: Structure of citizen's personal information.

For BD algorithm, the modified homogeneous second-order cone programming model is described as follows

$$\begin{pmatrix} X \\ P(X) \end{pmatrix} = \left\{ \begin{array}{c} a_1, a_2, \dots, a_m \\ p(a_1), p(a_2), \dots, p(a_m) \end{array} \right\}. \quad (6)$$

In which $0 \leq p(a_i) \leq 1$ ($i = 0, 1, 2, m$) and $\sum_{i=1}^m p(a_i) = 1$. The constant factor a_{ii} represents the $i * i$ value of the positive semidefinite matrix A of the homogeneous second-order cone programming model, and the information entropy in the data feature space is obtained as follows

$$H(X) = E(I(a_i)) = - \sum_{i=1}^m p(a_i) \log_2 p(a_i). \quad (7)$$

There are n samples in the data sample set S in the modified homogeneous second-order cone programming model, then

$$Q = \begin{bmatrix} 0 & y_1 & \cdots & y_n \\ y_1 & Q_{11} & \cdots & Q_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ y_n & Q_{n1} & \cdots & Q_{nn} \end{bmatrix} \stackrel{\text{def}}{=} \begin{bmatrix} 0 & y^T \\ y & Q \end{bmatrix}. \quad (8)$$

Based on the data preprocessing constructed by the characteristic information flow model of BD, the data algorithm is designed. In the traditional method, the linear dual cone programming method is used for the second-order cone programming model of BD, which has poor performance in data path tracking.

4. Definition of Citizens' Personal Information under BD

"Personal information" literally means all information related to citizens' personal body, identity, and activities. In an era of underdeveloped networks, I may only realize that my name,

address, ID number, and bank deposit password are important personal information, or that phone numbers fall into this category. People use ID cards to handle phone cards in the new network and BD era, and phone numbers are no longer just a string of numbers, but are tied to personal identity. First and foremost, it must be stated that not all citizens' personal information is protected under Chinese law. The legal concept of "citizens' personal information" differs from that of "personal information" in the broad sense, in terms of what information should be included in the scope of "citizens' personal information" protected by law. As a result, the personal information discussed below is all based on this. A large number of single recorded data are decomposed and combined to form a BD chain in the era of big data, and personal privacy is also exposed. People gradually adapt to digital life in the digital environment of BD construction, and personal privacy has changed in space, moving toward virtualization and digitalization. "Identifiable, distinguishable, confidential and semi-public information materials related to a specific person" is how we define "citizen's personal information." The contents covered therein are shown in Figure 2.

People gradually adapt to digital life in the BD construction environment, and personal privacy has changed in space, moving toward virtualization and digitalization. Furthermore, during the information age, various network platforms arose, developed quickly, and gradually penetrated people's daily lives, resulting in a large amount of new personal data. For instance, various information is generated when people carry out daily activities on various life service apps: the game account registered for playing games; track information generated by hotel and air ticket bookings; ordering takeout, online shopping, and stored preference information; capital account generated by stock speculation and investment; and so on. Furthermore, since the implementation of the "real name system," the rate of identity information utilization has improved, and various data related to personal identity are forming. The flow chart of administrative law protection of BD citizens' personal information is shown in Figure 3.

BD is an intellectual resource based on a large number of diverse and valuable data sets, which is formed through

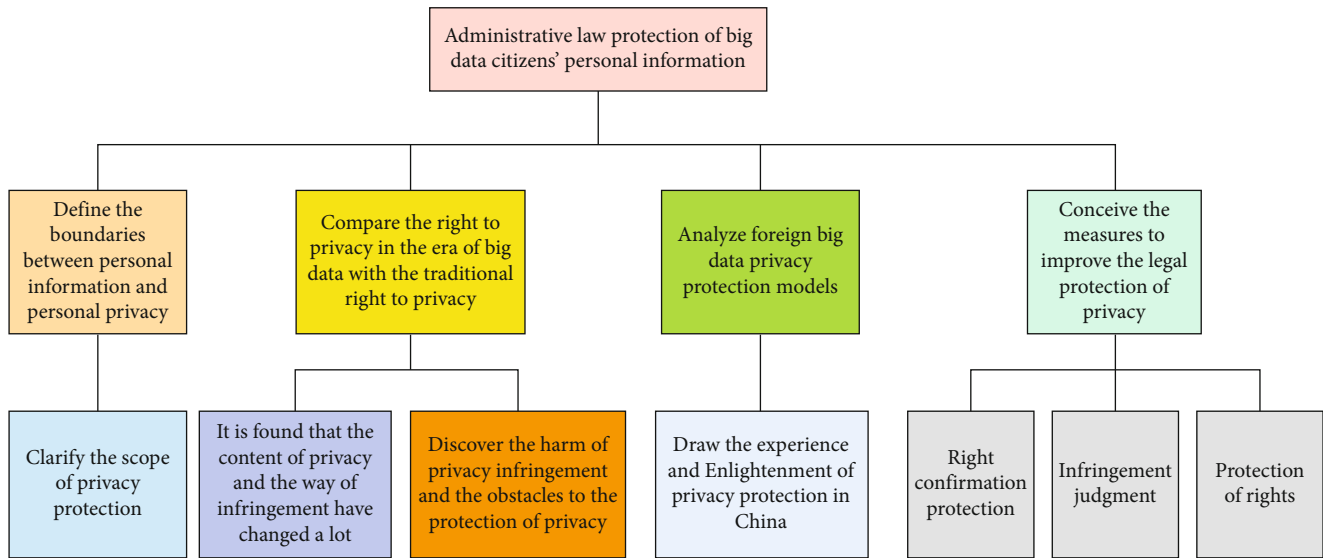


FIGURE 3: Flow chart of administrative law protection of BD citizens' personal information.

various data processing, analysis, and application. It is a brand-new technical architecture and service form. Zhong Wang, a well-known Chinese scholar, pointed out in his book *Privacy Regulation of Personal Data in the Age of BD* that the increase of data types and the expansion of data scale often only involve the level of traditional significance. BD also includes the collection and research of new information and the use of BD analysis technologies such as cloud computing and cloud storage to obtain commercial value from a large amount of information. As a combination of massive information and diversified information, BD contains enormous economic and social value, and almost all countries, regions, and all walks of life are keen on exploring, developing, and utilizing it. With the development of BD technology, the phenomenon of privacy infringement has become more and more serious. Massive data analysis has mined and reorganized the personal information of thousands of information subjects, exposing the privacy that was intended to be concealed to the sun. Privacy infringement in the era of BD has caused countless damages to the audience. It can be said that the concept of "personal information" is constantly updated with the development of the times, and it also reflects that our legislation attaches importance to citizens' personal information and keeps pace with the times. However, due to the different definitions of "citizen's personal information" in Chinese legislation and judicial interpretation, it is necessary to explore the connotation of "personal information" from different angles according to legislation and judicial interpretation, so as to obtain the real personal information protected in criminal law.

5. Suggestions on Perfecting the Administrative Law Protection of Citizens' Personal Information

5.1. Administrative Law Protection of Citizens' Personal Information Based on BD Analysis. China has scattered pro-

visions on personal information protection in various departmental laws, but there is a certain gap between the lack of coordination between departmental laws and the formation of a comprehensive protection system. The unified legislative model is more in line with the legislative tradition of China's statute law, and compared with the scattered legislative model, the unified legislation can effectively avoid the disadvantages of various standards and is more conducive to the effective implementation in judicial practice. In the era of BD, cases of personal information infringement emerge one after another, and the ways of personal information infringement are strange, but the law inherently lags behind. In order to overcome the problem of no legal rules to follow when there are loopholes in legal rules, enriching the corresponding legal principles has become a necessary measure to solve this problem. The powerful information mining and analysis ability of BD technology makes people's privacy more vulnerable to illegal infringement. In the era of BD, the means of infringement are more scientific and technological, and the way for infringers to steal people's privacy is gradually transferred from real space to virtual network carrier. Two departments are set up for different supervision objects to supervise administrative organs and nonadministrative organs, respectively, and give them corresponding administrative powers, such as investigation and inspection power, administrative adjudication power, administrative punishment power, and administrative relief power.

Under the background of BD, the protection rules of citizens' personal information administrative law are not perfect. With the development of the era of BD, private space is no longer just the traditional private real space, but also private virtual space begins to appear. Private space refers to the personal privacy field recorded in the form of data, including our common software such as QQ mailbox, QQ space, WeChat circle of friends, voice call, and short message transmission of electronic devices. All belong to the category of private virtual space and should be effectively protected. In the era of BD, more emphasis is placed on the

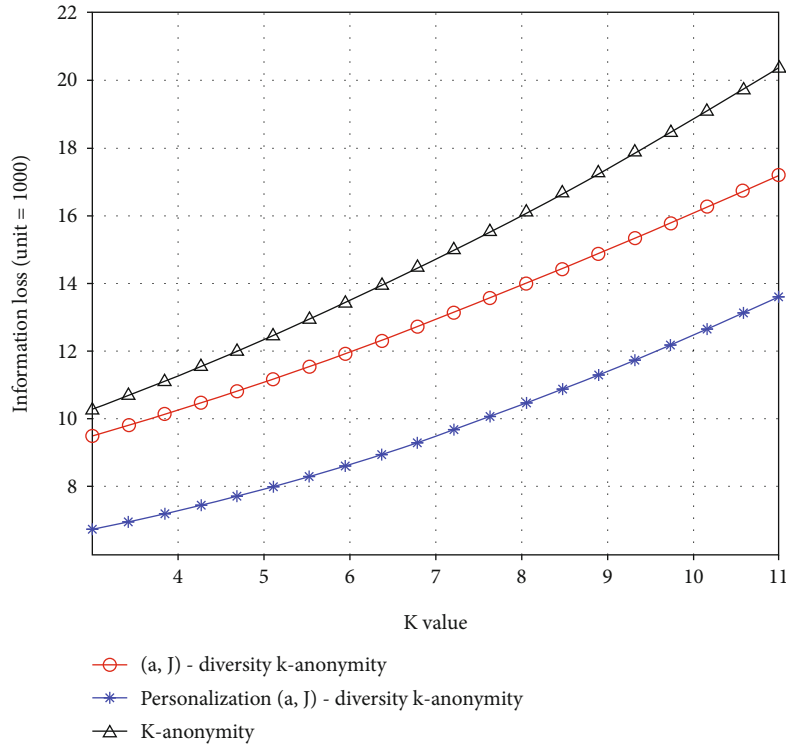


FIGURE 4: Information loss under different k values.

information recorded in the virtual space of the network, such as the personal whereabouts track found by the positioning system and the status of network property. This information is closely related to individuals, and once leaked, it will cause huge loss of personal property, so the law needs to strengthen the protection of this content. Finally, we should establish a scientific personal information administrative supervision system. According to the closeness of personal information and the privacy level of personal information, citizens' personal information is divided into four categories: personal information, personal sensitive information, direct identification information, and indirect identification information, and different protection efforts are determined according to different categories.

5.2. Experimental Results and Analysis. The experimental data in this paper comes from the UCI machine learning warehouse's adult data set, which is widely used in the privacy protection field. There are 48756 records in the dataset. To obtain a dataset with 31269 records, remove the records with null values and uncertain information. The information loss under the three privacy models occurs when the data set size is 316569 records and the K value changes. As a result, the personal information discussed further down is all based on this. A large number of single recorded data are decomposed and combined to form a BD chain in the era of big data, and personal privacy is also exposed. For instance, various information is generated when people carry out daily activities on various life service apps: the game account registered for playing games; track information generated by hotel and air ticket bookings; ordering takeout, online shopping, and stored preference information; capital account

generated by stock speculation and investment; and so on. Because it increases the personalized protection of sensitive values, the information loss of the diversity k -anonymity model is greater than that of the other two models, as shown in Figure 4.

Figure 4 shows the comparison of information loss among the three models when $k=5$ and the data set size change. It can be seen that with the increase of data set size, the information loss of anonymous data sets under the three models is increasing. Because with the more records that need to be anonymized, the number of attribute values that need to be processed will correspondingly increase, thus, the greater the amount of information loss. The information loss of data set under k -anonymous model is always less than the other two because this model only restricts the size of equivalent groups. However, because it increases the anonymity operation for some sensitive attribute values, as shown in Figure 5.

Figure 5 depicts the recognition rate of sensitive values under the three privacy models when the K value changes against the same data background. It can be seen that as the K value increases, the average recognition rate of sensitive values of data sets decreases in all three models. Furthermore, since the implementation of the "real name system," the rate of identity information utilization has improved, and various data related to personal identity are forming. With the advancement of BD technology, the problem of privacy invasion has become increasingly serious. As a result, when compared to the other two models, the sensitive value recognition rate is always the lowest, and the privacy protection effect is always the best, as shown in Figure 6.

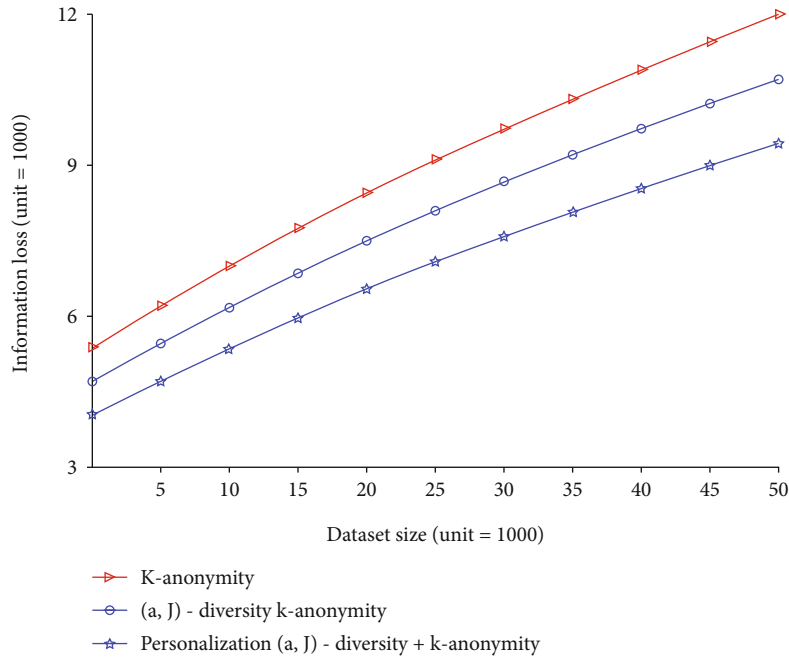


FIGURE 5: Information loss under different data set sizes.

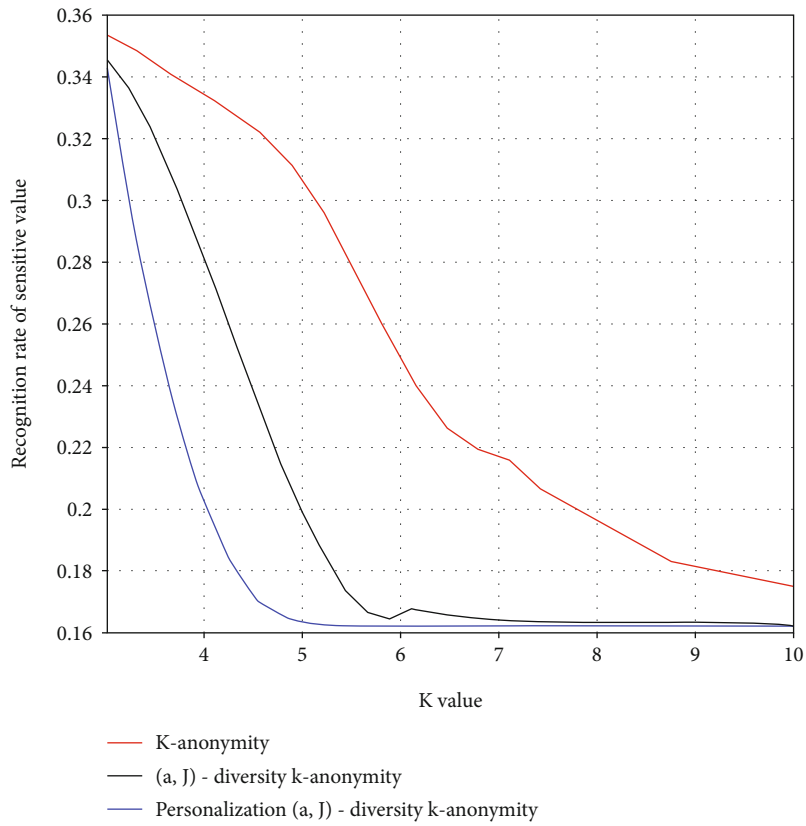


FIGURE 6: Identification rate of sensitive values under different K values.

Figure 6 shows the comparison of sensitive value recognition rate under different data sets with $k = 5$. It can be seen that the change of data set size has little effect on the overall

recognition rate of sensitive values under the three models. Massive data analysis has mined and reorganized the personal information of thousands of information subjects,

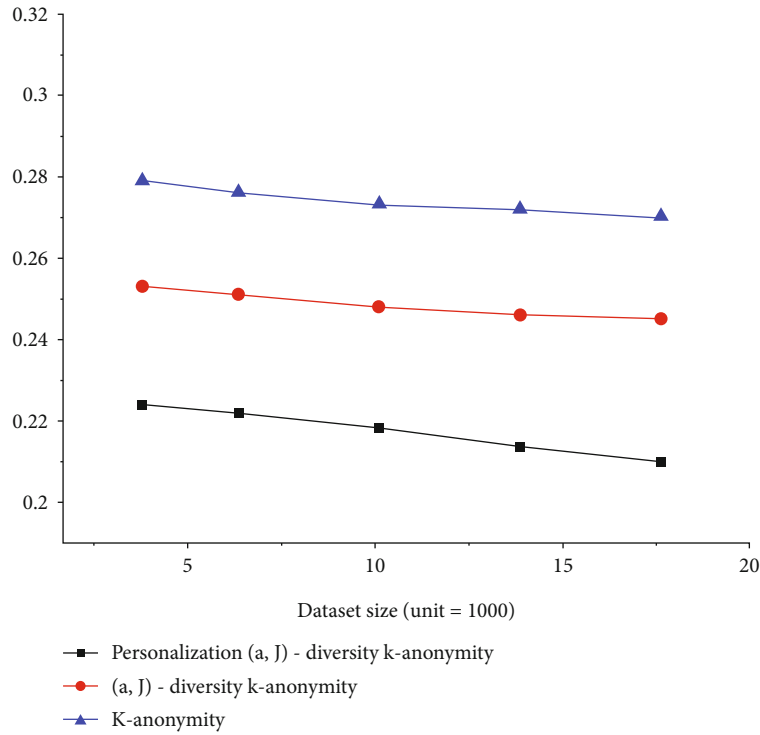


FIGURE 7: Identification rate of sensitive values in different data sets.

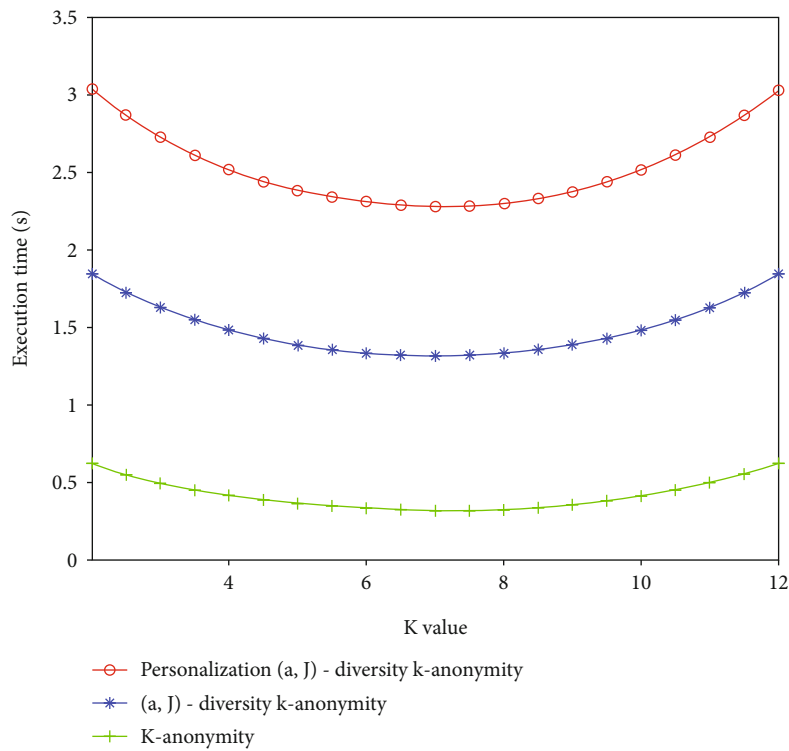


FIGURE 8: Execution time under different K values.

exposing the privacy that was intended to be concealed to the sun. Privacy infringement in the era of BD has caused countless damages to the audience, as shown in Figure 7.

Figures 8, 9 and 10, respectively, compare the running time of the three models under the change of k value and data set size. In Figure 8, when the value of k changes, the

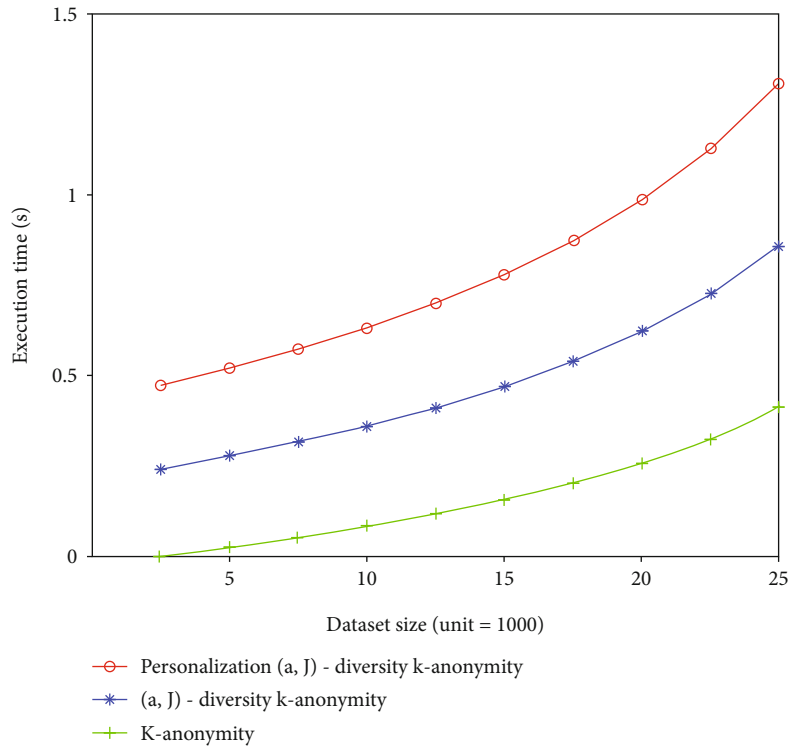


FIGURE 9: First execution time under different data set sizes.

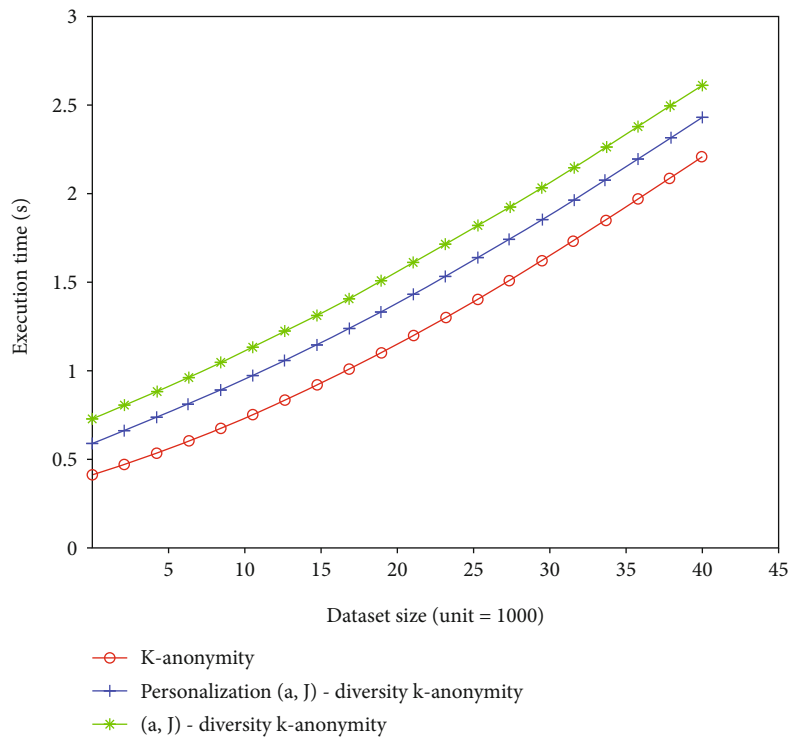


FIGURE 10: Second execution time under different data set sizes.

running time of the three models fluctuates to some extent. The development history of the administrative law protection of citizens' personal information has been for many years. The traditional citizens' personal information pays

attention to the tranquility of citizens' personal life alone, and the maintenance of citizens' personal information is actually to protect citizens' personal freedom, dignity, and happy tranquility. With the continuous improvement and

popularization of the Internet, the right to privacy of BD has more new meanings, and the means of administrative law protection of citizens' personal information have become diverse. Obviously, because the random selection of initial tuples when dividing equivalence groups will affect the experimental results of each model.

Only when the peace of private life is invaded does the disclosure of personal information infringe on privacy. Personal data and privacy are linked in some ways. Clarifying the difference between the two is the first step in creating a perfect privacy protection system. In practice, some administrative organs have violated citizens' personal information when exercising administrative power, but the relevant collection of personal data lacks the necessary compliance judgment due to a lack of relevant theories. Furthermore, China's legal system for personal data protection needs to be improved as a whole. For example, in the era of "BD," the definition of personal information is not unified and qualitative, the subject of responsibility in cyberspace is unknown, and the behavior of infringing personal information in various fields is complex and varied, resulting in the ineffectiveness of personal information protection measures.

6. Conclusion

To summarize, use administrative power to strengthen personal data protection, clearly define the basic content of citizens' personal data, as well as the power scope and types of power subjects, expand the functional scope of regulatory agencies, improve the regulatory mechanism, and implement the later construction of an economic relief system. The demand for data information is growing, and the quality of personal information is becoming increasingly important. Administrative bodies and social organizations will inevitably infringe on the rights of information subjects in the pursuit of public and private interests. Of course, because there is no special legislation on personal information protection in China, criminal ancestors have become the current situation of personal information protection in order to crack down on crimes in a timely manner. The pace of protection of China's personal information right is slow precisely because of the lack of restraint and control of relevant laws and regulations. Administrative organs are not supervised when performing their functions precisely because of the lack of protection provided by administrative regulations. The current abuse of power has resulted in contradictions and differences between the exercise of administrative functions and the protection of citizens' personal information rights. Solving this problem from the perspective of administrative law can not only resolve contradictions and balance the interests of both sides but also be a major innovation and bright spot in the legal protection system.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The author does not have any possible conflicts of interest.

Acknowledgments

This study was supported by (1) The Project of Teaching Quality and Teaching Reform of University of Electronic Science and Technology of China Zhongshan Institute: Online open course of Administrative Law and Administrative Litigation Law (Project number: SKC202001); and (2) the Guangdong Teaching Quality and Teaching Reform Project: Administrative Law and Administrative Litigation online course (course no. ZXKC202007).

References

- [1] R. Akdoğan and E. Çimşir, "Linking inferiority feelings to subjective happiness: self-concealment and loneliness as serial mediators," *Personality and Individual Differences*, vol. 149, pp. 14–20, 2019.
- [2] J. Lin, L. Carter, and D. Liu, "Privacy concerns and digital government: exploring citizen willingness to adopt the COVID-Safe app," *European Journal of Information Systems*, vol. 30, no. 4, pp. 389–402, 2021.
- [3] S. Spiekermann and J. Korunovska, "Towards a value theory for personal data," *Journal of Information Technology*, vol. 32, no. 1, pp. 62–84, 2017.
- [4] L. W. Zaseck, N. R. Orton, R. Gruber et al., "The influence of personal protection equipment, occupant body size, and restraint system on the frontal impact responses of Hybrid III ATDs in tactical vehicles," *Traffic Injury Prevention*, vol. 18, no. 6, pp. 642–649, 2017.
- [5] E. S. Dove and J. Chen, "To what extent does the EU general data protection regulation (GDPR) apply to citizen scientist-led health research with mobile devices?," *The Journal of Law Medicine & Ethics*, vol. 48, no. S1, pp. 187–195, 2020.
- [6] J. Holbein, *Left Behind? Citizen Responsiveness to Government Performance Information*, American Political Science Association, 2016.
- [7] H. N. Chua, S. F. Wong, Y. Chang, and C. F. Libaque-Saenz, "Unveiling the coverage patterns of newspapers on the personal data protection act," *Government Information Quarterly*, vol. 34, no. 2, pp. 296–306, 2017.
- [8] R. H. Hariri, E. M. Fredericks, and K. M. Bowers, "Uncertainty in big data analytics: survey, opportunities, and challenges," *Journal of Big Data*, vol. 6, no. 1, pp. 1–16, 2019.
- [9] F. Caputo, V. Cillo, E. Candelo, and Y. Liu, "Innovating through digital revolution," *Management Decision*, vol. 57, no. 8, pp. 2032–2051, 2019.
- [10] Y. Suda, "Japan's personal information protection policy under pressure," *Asian Survey*, vol. 60, no. 3, pp. 510–533, 2020.
- [11] F. Costa-Cabral and O. Lynskey, "Family ties: the intersection between data protection and competition in EU law," *Common Market Law Review*, vol. 54, no. 1, pp. 11–50, 2017.
- [12] F. Borgesius, "Singling out people without knowing their names - behavioural targeting, pseudonymous data, and the new data protection regulation," *Computer Law & Security Review*, vol. 32, no. 2, pp. 256–271, 2016.

- [13] A. Meijer and S. Potjer, "Citizen-generated open data: an explorative analysis of 25 cases," *Government Information Quarterly*, vol. 35, no. 4, pp. 613–621, 2018.
- [14] S. W. Dagan, A. Ben-Porat, and H. Itzhaky, "Child protection workers dealing with child abuse: the contribution of personal, social and organizational resources to secondary traumatization," *Child Abuse & Neglect*, vol. 51, pp. 203–211, 2016.
- [15] E. Soukiazis and S. Ramos, "The structure of subjective well-being and its determinants: a micro-data study for Portugal," *Social Indicators Research: An International and Interdisciplinary Journal for Quality-of-Life Measurement*, vol. 126, no. 3, pp. 1375–1399, 2016.
- [16] A. T. Chatfield and C. G. Reddick, "All hands on deck to tweet #sandy: networked governance of citizen coproduction in turbulent times," *Government Information Quarterly*, vol. 35, no. 2, pp. 259–272, 2018.
- [17] A. Malatras, I. Sanchez, L. Beslay et al., "Pan-European personal data breaches: mapping of current practices and recommendations to facilitate cooperation among data protection authorities," *Computer Law & Security Review*, vol. 33, no. 4, pp. 458–469, 2017.
- [18] X. L. Meng, "Statistical paradises and paradoxes in big data (I): law of large populations, big data paradox, and the 2016 US presidential election," *The Annals of Applied Statistics*, vol. 12, no. 2, pp. 685–726, 2018.
- [19] B. Tang, Z. Chen, G. Hefferman et al., "Incorporating intelligence in fog computing for big data analysis in smart cities," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2140–2150, 2017.
- [20] X. Luo, L. Dong, Y. Dou et al., "Analysis on spatial-temporal features of taxis' emissions from BD informed travel patterns: a case of Shanghai China," *Journal of Cleaner Production*, vol. 142, Part 2, pp. 926–935, 2017.
- [21] P. Baltiiski, I. Iliev, B. Kehaiov, V. Poulkov, and T. Cooklev, "Long-term spectrum monitoring with big data analysis and machine learning for cloud-based radio access networks," *Wireless Personal Communications*, vol. 87, no. 3, pp. 815–835, 2016.
- [22] K. S. Cheung, W. K. Leung, and W. K. Seto, "Application of big data analysis in gastrointestinal research," *World Journal of Gastroenterology*, vol. 25, no. 24, pp. 2990–3008, 2019.
- [23] P. K. Lorgelly, B. Doble, and R. J. Knott, "Realising the value of linked data to health economic analyses of cancer care: a case study of cancer 2015," *Pharmacoeconomics*, vol. 34, no. 2, pp. 139–154, 2016.
- [24] N. An and X. Wang, "Legal protection of artificial intelligence data and algorithms from the perspective of internet of things resource sharing," *Wireless Communications and Mobile Computing*, vol. 2021, no. 2, Article ID 8601425, 10 pages, 2021.