



Analyzing the Legal System for Protecting Workers' Health and Privacy Based on Collaborative CAD and Big Data

Yuxia Gao ¹*

¹ Zhengzhou Sias University, Henan 451100, China

Corresponding author: Yuxia Gao, gaoyuxia0318@126.com

Abstract. China's labor legislation only focuses on protecting workers' employment environment and working conditions, emphasizing the protection of workers' material interests and material personality rights while ignoring the protection of workers' personality rights and interests. Therefore, this paper further analyzes the legal system of protecting workers' health and privacy based on big data in the network information environment. After adding privacy, the selected features still come from the original grouping, so the classification accuracy will not change much, which can protect the privacy of features. Under the network information environment, taking the legal protection of workers' privacy rights as the research theme, answering the main existing problems and the ways to solve them, respecting their fundamental personality rights as the improvement direction, and coordinating the relationship between workers and employers.

Keywords: Network information; Big data; Protection of workers' health privacy; Legal system; Collaborative CAD

DOI: <https://doi.org/10.14733/cadaps.2025.S5.165-177>

1 INTRODUCTION

In China, the development of civil law is relatively slow, the research on the right to privacy is lagging, and the legal protection of the right to privacy is relatively weak. However, with the development of social civilization and legal systems, citizens' awareness of respecting others' privacy and self-privacy is growing. China's civil law has experienced a tortuous process, from never recognizing the right to privacy to confirming the right to privacy [4]. As China is still in the primary stage of socialism, economic interests remain the workers' primary concern. Therefore, China's labor legislation only focuses on protecting workers' employment environment and working conditions, emphasizes the protection of workers' material interests and material personality rights, and ignores protecting workers' personality rights. Since the reform and opening up, due to the needs of national economic development, the administrative work and legislative protection of

the labor department in China tend to ensure the smooth progress of productive labor. In contrast, the protection of workers' health privacy has progressed slowly. There are still many deficiencies in the legal protection of workers in China [14],[1]. In the dynamic evolution of work environments, the convergence of technology, big data, and the well-being of employees has emerged as a pivotal area of concern and potential advancement. With industries progressively immersing themselves in the landscapes of Collaborative CAD, the legal structures designed to safeguard workers' health and privacy are encountering novel and complex challenges. This examination intricately navigates the dynamics involved in ensuring the protection of employees within the information environment, scrutinizing the ramifications of employing big data within the framework of occupational health and privacy laws. Although Article 8 of the Contract Law relates to the right to privacy of workers and restricts the right to know of employers, which provides specific legal protection for the protection of workers' right to privacy, the user unit may abuse this right in labor relations and infringe on workers' interests in a legal name because it fails to make more specific provisions on workers' right to privacy. Therefore, improving the legal protection of workers' privacy is urgent.

With the continuous development of the market economy, advanced technology and science have changed the traditional mode of production and brought new health problems. Only the daily supervision and management of the labor law enforcement department has been far from ensuring the realization of workers' health rights and interests [6]. This paper conducts research on the legal system of workers' health privacy protection based on big data in the network information environment, deeply analyzes the content of workers' privacy involved in labor relations and the types and manifestations of common violations of workers' privacy, tries to put forward principles and legislative suggestions for improving the legal protection of workers' privacy, and puts forward some ideas for improving the legal protection of workers' privacy [10],[2]. The network environment is not impeccable. Network activities are interactive and transparent. In the network environment, our activities are almost omnidirectional. This characteristic of the network brings significant challenges to the network users who lack the awareness of privacy protection. A little carelessness will lead to the infringement of the right to privacy, but they do not know it.

In labor relations, subordination is one of the most essential characteristics of labor relations between workers and employers. After a worker establishes a labor relationship with an employer, the employer often infringes on the worker's right to privacy due to its need to exercise management power and its economic advantage, thus triggering a conflict between the worker and the employer [18],[17]. Strengthening the protection of the right to network privacy conforms to the trends of the times, meets the public's requirements for a more secure network environment, and promotes the development of the Internet industry. In terms of its essence, the right to privacy is to define the relationship between personal affairs and social public interests. The law needs to protect individual privacy based on the protection of personal dignity and personal freedom. However, the law needs to make necessary restrictions on personal privacy from the perspective of safeguarding social and public interests. The cases of Chinese employers' infringement of workers' privacy are also on the rise yearly. Workers' privacy cannot be effectively protected, and the legal accountability system for employers is not sound. Therefore, this paper combines the network information environment, takes the legal protection of workers' privacy as the research topic, summarizes the current legislative status of the legal protection of workers' privacy in China, answers the main problems and ways to solve them, respects their fundamental personality rights as the perfect direction, and coordinates the relationship between workers and employers.

Innovation content:

It analyzes the current situation of the legal protection of workers' privacy. The protection of human privacy has incalculable value. Therefore, except for countries that are above individuals,

no one has any reason to deprive or damage the privacy of others, no matter what their purposes or rights are.

II This paper constructs the system by analyzing the legal system of protecting workers' health privacy in the network information environment. In labor relations, the employer, under the network information, based on normal operation and management needs, advocates exercising its right to know and understand better or master the relevant information of workers, which is in line with the law and reasonable.

The overall structure of this paper consists of five parts.

The first chapter describes the background and significance of workers' health privacy protection. The second chapter mainly introduces the research summary of protecting workers' health privacy. The third chapter analyzes the content related to workers' privacy in labor relations and proposes the necessity of workers' privacy based on big data. Finally, it studies the legal system of workers' health privacy protection under the network information environment. The fourth chapter is the experimental part. The fifth chapter is the summary of the full text.

2 REVIEW OF RESEARCH

The right to privacy is a fundamental personality right enjoyed by natural persons. As natural people, workers should also enjoy the right to privacy. Scholars' research on workers' right to privacy is still in its infancy, and different theorists have studied it from various angles. The right to worker privacy has also formed different concepts.

Cho H, et al. pointed out that human rights include many aspects: the right to security, freedom, politics, etc. Therefore, relative to workers, labor rights are equal to workers' human rights. Workers' occupational health rights and interests are the concrete manifestation of workers' right to life, which is related to workers' life health and life security and directly refers to workers' pursuit of the minimum right to life so that human beings can meet their psychological and physiological needs [5]. Bhavé D P et al. put forward the problem of differentiated protection of workers' privacy rights. It is argued that different occupations have different occupational safety risks, so workers' privacy rights should be restricted to different degrees according to the characteristics of different posts [3]. Moore W et al. think that it can be done in the following ways: is the scope that the employer can intervene in the employee's privacy outside the workplace through consultation between the employer and the employee; Second, the dual protection mechanism is adopted; workers can get not only limited protection in the workplace but also get comprehensive protection outside the workplace [15]. De Stefano V believes that the so-called employee's right to privacy refers to a kind of personality right that the employee controls his personal information, private activities, and private fields that are not related to the productive activities of the employer before, during, and after the establishment of the labor relationship and the termination of the labor relationship [7]. Van Kolschooten H et al. show that the protection of workers' health privacy, as a basic form of human rights, reflects the respect for human life value, and the protection of workers' occupational health is also the protection of workers' human rights and labor rights. What's more critical is employers' and employees' different interests and value pursuits. The comprehensive protection of workers' occupational health can't be accomplished through the contract form of private law [19]. Kitsiou A. et al. pointed out that from the scope of protection, it is a right that personal privacy and private information are protected by law from being illegally invaded, known, collected, utilized, and disclosed by others. The scope of protection includes two aspects [12]. Namara M et al. put forward that the essence of protecting workers' occupational health rights is to find a balance between employers' interests and workers' interests, to prevent employers from excessively pursuing interests and neglecting or damaging workers' interests, and to provide legal protection for workers to protect themselves [16]. Zuiderveen

Borgesius F J believes there are some differences between the relevant legislation in the civil field and the legislative ideas in the labor law field, which can't reflect the problems existing in protecting workers' privacy rights. Therefore, a protection system that conforms to the legislative ideas of labor law should be formulated [22]. Feng Q et al. proposed that protecting workers' privacy not only exists during labor relations but also extends the scope of protection to before the formal establishment of labor relations and after the termination or dissolution of labor relations. However, its improper place lies in excluding the privacy rights enjoyed by workers related to the production activities of employers. However, under certain circumstances, workers should transfer part of their privacy rights for the public interest or employers' more significant economic interests [8]. Yazdinejad A, et al. expounded on the considerable changes in business, management, and big thinking in the era of big data, in which the most significant risk of management change is to bring a significant crisis to privacy. At the same time, the current development situation points out new problems in protecting workers' privacy rights. It predicts the possible changes and security problems in the future big data environment [21].

3 RESEARCH METHOD

3.1 Contents Involving Workers' Privacy in Labor Relations

The workers' personal information is unique, mainly manifested in that the employer has the right to obtain some personal information; the law gives the employer the right to know about workers' personal information appropriately. The content of the right to know can be divided into five aspects: knowing the political power. Social right to know, The right to know personal information, Legal right to know, and Employers' right to know [11],[20]. It includes the employer's knowledge of the relevant information of its internal members and the members who will join its organization. Laborers are a specific social concept and social group, and labor rights can be seen as a particular human right of workers to a certain extent. First, labor rights are an essential component of human rights. From the perspective of the subject and content of the labor right, the absence of the labor right will lead to the imperfection of human rights [13]. Second, as a fundamental human right, the value of labor rights is the pursuit and realization of material interests and human value and dignity. Therefore, the most significant difference from the traditional era is that violating the right to privacy has damaged human dignity and the loss of property interests. The rapid development of the information society makes the traditional protection model of the right to privacy lose effectiveness and can not adapt to it. The above analysis shows the status quo of legal protection of workers' privacy in Figure 1.

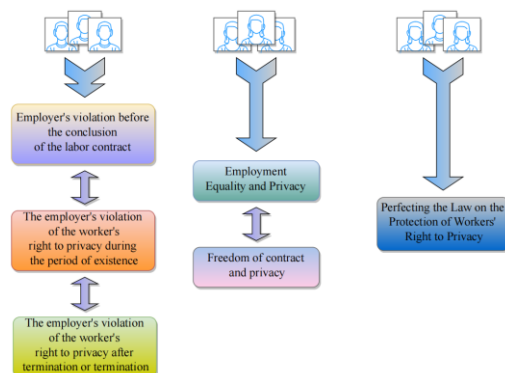


Figure 1: Status quo of legal protection of workers' privacy rights.

Regarding the concept of privacy, there are mainly the following definitions in academic circles: First, it is considered that privacy is the freedom individuals enjoy to control their private lives; Second, the right to privacy is a right to keep individuals alone without interference [9]. The law gives employers the right to know because employers, as investors of enterprises and managers of production and operation, primarily aim to make profits. People's privacy protection has immeasurable value. Therefore, no matter what purpose or right anyone has, there is no reason to deprive or damage other people's privacy, except for countries that are above the individual. Compared with workers, privacy protection is the bottom line. Therefore, employers must protect workers' privacy as the starting point in daily management to fully realize workers' human rights. Employers can't expand their right to know indefinitely, and some unnecessary personal private information should not be included in the scope of employers' right to know.

In addition to basic information, workers' personal information also has deep information, which individuals generally do not want to be known by outsiders and should belong to the scope of secret information. This shows that protecting workers' privacy is the fundamental right of human existence, the primary and essential content of personality rights, and the highest personal interests of citizens. Privacy protection is the concrete expression of workers' privacy security, and it is the personal interest that workers can enjoy with their own life and privacy as the object.

3.2 Necessity of Workers' Privacy Based on Big Data

Big data refers to data collection that cannot be captured, managed, and processed with conventional software tools within a specific time frame. It is a massive, high growth rate and diversified information asset that requires a new processing mode for more substantial decision-making power, insight and discovery, and process optimization energy. Big data turns data into valuable conclusions through collecting, managing, and in-depth mining of personal information. At the same time, it also uses cutting-edge technology to penetrate all aspects of people's lives, leaving citizens with nowhere to hide their privacy. The degree of disclosure of citizens' personal information and privacy has also been several times as before. Therefore, this paper analyzes the workers' privacy rights based on big data. Information on the basic level belongs to the applicants or workers who must disclose to the enterprise, and information on the depth level belongs to the applicants or workers who have the right to refuse to disclose as "privacy." For example, the marital status of employees belongs to the primary level. In contrast, the emotional life of married people, the marriage plan of unmarried people, the reasons for divorce, and the reasons for widowhood all belong to the depth level of personal information in big data. Another example is the employee's family genetic disease. The employer only needs to know the nature and hidden danger of the disease and has no right to ask about the causes of such diseases among the employees' family members.

As workers spend most of their time in the workplace, in addition to their labor behavior, they are also inevitably engaged in some private activities, such as answering private phones or having private conversations with colleagues. This paper is based on the data form processed by big data privacy protection, some pre-processing measures for data before implementing privacy protection, and some calculation methods to measure data dissimilarity. Indicators represent each object to show its characteristics:

$$X_i = (x_{i1}, \dots, x_{in}) \quad (1)$$

Thus, the original data matrix is:

$$\begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ \dots & \dots & \dots & \dots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \quad (2)$$

Set the value v of attribute A to v' after conversion

$$v' = \frac{v - \min A}{\max A - \min A} \quad (3)$$

The v' of attribute A value v after conversion is:

$$v' = \frac{v - \bar{A}}{\sigma_A} \quad (4)$$

Where A and σ_A refer to the mean and standard deviation of attribute A respectively.

The dissimilarity between objects is generally calculated based on the distance between objects. The most common distance measurement methods are:

Euclid distance

$$d(i, j) = \sum_{k=1}^n x_{jk}^2 \quad (5)$$

Manhattan distance

$$d(i, j) = \sum_{k=1}^n x_{jk} \quad (6)$$

The above two distances are special cases of Minkowski distance, which is described as follows:

$$d(i, j) = \sum_{k=1}^n x_{jk}^q \quad (7)$$

Where q is a positive integer when $q = 1$ represents the calculation formula for the Manhattan distance; when $q = 2$, it means the Euclid distance calculation formula.

These belong to the scope of workers' privacy and are inviolable. With the arrival of the age of big data and the popularization of technology, workers' information will be more and more widely involved in the data age. At a time when technology and legislation are not perfect, the possibility of data leakage, information, and privacy violations is also significantly increased. Although, as the owner of the workplace and the manager of production and operation, employers order to safeguard their interests and improve work efficiency, There is nothing wrong with supervising the production activities of workers in a certain way, but this does not mean that the employer has the right to monitor all the activities of workers. The employer has the right to supervise only the labor behaviors of workers, as well as private behaviors that are irrelevant to the labor behaviors of workers or are implemented during non-labor hours. Therefore, forming a sound legislative system to match big data technology's development speed and trend is imperative.

3.3 Research on the Legal System of Workers' Health Privacy Protection Under the Information Environment

From the workers' point of view, they demand that their private lives and space should not be illegally interfered with by others to obtain peace of mind and maintain their independence and dignity. From the perspective of employers, workers themselves are one of the significant wealth of employers, and the quality of workers directly affects their economic benefits. In labor law, when the public's right to know conflicts with workers' right to privacy, workers' behavior of transferring some personal privacy to satisfy the public's right to know reflects this point. To avoid the loss to the other party caused by the coordination of rights, in practice, it is necessary to clarify the scope of the public's right to know and the scope of workers' privacy by legislation. There is no essential difference between online privacy and traditional privacy. It still belongs to a kind of privacy and has the general attribute of privacy. The subject of the right is a natural person, and the content of the right involves the peace of private life, confidentiality of information, confidentiality of communication, and independent use of privacy. The right to privacy

on the Internet has become one of the most significant legal issues, and the right to privacy has also become a fundamental right that occupies an essential position in Internet law. In the current network society, people communicate and seek all kinds of information with virtual identities, but there is no real physical contact, and people's materiality is hidden. The demand for personal information in society shows an infinite expansion trend in the network information environment. As an essential part of information, the economic value of workers' health privacy is also increasing, and the probability of being infringed is growing faster. Therefore, in addition to the negative content, the positive content of workers' right to health and privacy under the network environment also occupies the leading position. The primary purpose of legal protection of privacy rights is to protect the peace of life and the undisturbed private life. At the same time, the legal protection of network privacy rights is also meant to guarantee the domination of network privacy rights and enhance the nature of their rights. After studying the legal system of protecting workers' health and privacy in the network information environment, a systematic diagram of the legal system of protecting workers' health and privacy in the network information environment is proposed, as shown in Figure 2.

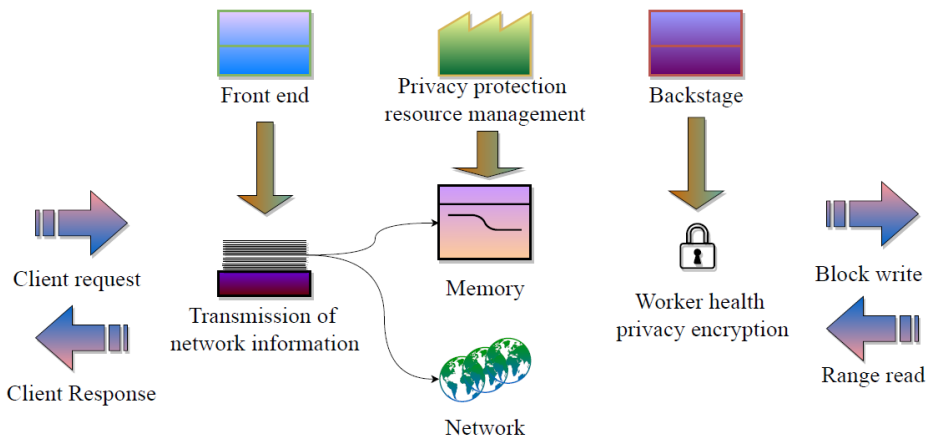


Figure 2: Legal system diagram of network information environment for workers' health privacy protection.

In labor relations, the employer, under the network information, based on the regular operation and management needs, advocates to exercise its right to know and better understand or master the relevant information of workers, which is in line with the law and reasonable. However, exercising the right to know should also follow the principle of moderation to avoid unnecessary losses to workers. The conflict between the right to privacy of workers and the right to know of employers is mainly reflected in the process before and during the conclusion of labor relations. This distance plays a vital role in multivariate statistical analysis through the legal system of protecting workers' health privacy under the network information environment. The definition is given below.

Let the matrix represent Σ the covariance matrix of the index:

$$\Sigma = \sigma_{ij} \tag{8}$$

If summation exists for Σ^{-1} exists, the distance between the two samples is:

$$d^2(i, j) = (X_i - X_j) \quad (9)$$

The interference of the correlation among indexes is eliminated and not affected by the dimensions of each index.

It is used to calculate a Gaussian influence function:

$$f_{Gauss} = e^{-\frac{d(x,y)}{2\sigma^2}} \quad (10)$$

Or square wave influence function:

$$f_{square} = \begin{cases} 0 & \text{if } d(x, y) > \sigma \\ 1 & \text{if } d(x, y) \leq \sigma \end{cases} \quad (11)$$

According to the definition of influence function and the description of Gaussian influence function and square wave influence function, the clustering algorithm based on density is still to find the similarity between data, but its similarity is no longer measured by distance. Unreasonable or unsafe actions of workers in the specific operation process under the network information environment to serve the future staff training. Employers invest and organize production activities for profit, which is their natural legitimate interest and should be recognized and protected by law. Moreover, as the employer's private property, work, and production have the right to install the facilities, he is willing to install them on all his property according to the principle of ownership. The adequate protection of the right to privacy on the Internet can't be achieved without government supervision, and at the same time, government supervision also needs legal support. Strengthening government supervision can compensate for the deficiency of legal provisions and take timely and comprehensive precautions against the infringement of workers' health and privacy protection through network information. It also plays a positive role in promoting the long-term and healthy development of the network.

4 RESULT ANALYSIS AND DISCUSSION

The primary function of worker privacy protection is to store data. Encryption technology protects data and ensures data security in the system database. The public key in the password verification processing under the network information environment can verify the encrypted password. In this case, the asymmetric encryption algorithm is used to manage the key of the symmetric algorithm. Then, the symmetric encryption algorithm is used to encrypt the data, which can inherit the advantages of the symmetric and asymmetric algorithms and achieve better encryption processing. The experimental results are shown in Table 1 - Table 3.

<i>Field Name</i>	<i>Field Description</i>	<i>Field Type</i>
<i>ID</i>	<i>Number</i>	<i>NVARCHAR(17)</i>
<i>USERNAME</i>	<i>Name of worker</i>	<i>NVARCHAR(17)</i>
<i>BASE INFO</i>	<i>Essential information</i>	<i>NVARCHAR(110)</i>

Table 1: Employee privacy retrieval record.

Table 1 lists the main fields of the employee privacy search record form, including number, user name, user basic information, employee information, and privacy information. According to whether the searched employee information involves privacy, the system writes the information into the employee and privacy information fields, respectively.

<i>Field Name</i>	<i>Field Description</i>	<i>Field Type</i>
<i>ID</i>	<i>Number</i>	<i>NVARCHAR(17)</i>
<i>TITLE</i>	<i>Title of knowledge point</i>	<i>NVARCHAR(33)</i>

<i>TYPE</i>	<i>Category</i>	<i>NVARCHAR(33)</i>
-------------	-----------------	---------------------

Table 2: Information table of knowledge points.

<i>Field Name</i>	<i>Field Description</i>	<i>Field Type</i>
<i>ID</i>	<i>Number</i>	<i>NVARCHAR(17)</i>
<i>TITLE</i>	<i>Title Name</i>	<i>NVARCHAR(17)</i>
<i>TYPE</i>	<i>Category</i>	<i>NVARCHAR(33)</i>

Table 3: Warning education information table.

Table 2 lists the main fields of the knowledge point information table, including the title, category, and content of the knowledge point. Table 3 lists the main fields of the warning education information table, including the title, category, and content.

As the cluster evaluation indicators of worker privacy protection selected in this paper are all relative indicators, for the scalability of privacy protection, this paper uses four systems to analyze the relative proportion between the running time of the worker privacy protection legal mechanism and the amount of data, that is, the running time change degree, as shown in Figure 3. It can be seen from the experimental results that the system method in literature [6] has the worst scalability, followed by the system in literature [9] and then the system in literature [14]. However, the system proposed in this paper has the best privacy protection effect among the four systems.

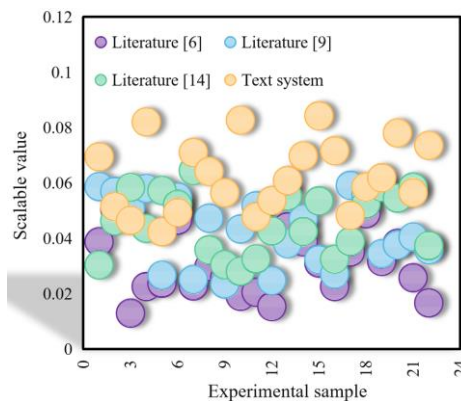


Figure 3: Statistical analysis results of scalable privacy protection algorithms in different systems.

As for the complexity of employee privacy protection in the system, it can be seen directly from the running time statistics of different privacy protection methods in the data set of Figure 4 that the system in reference [6] has the longest running time, followed by the system in reference [9]. Then, the system in reference [14] and the system built in this paper have the shortest running time. It can also be seen from the statistical analysis results of the privacy protection algorithm of running time in Figure 5 that the system in document [6] has the longest running time, followed by the system in document [9], and then the system in document [14], with the shortest running time being the system still constructed in this paper. The above two experiments further illustrate that references [6], [9], and [14] are not suitable for processing high-dimensional data sets. For all kinds of sampling methods, the method in this paper has a relatively low operation time for the sampling method of protecting workers' privacy, so it can also process high-dimensional data sets.

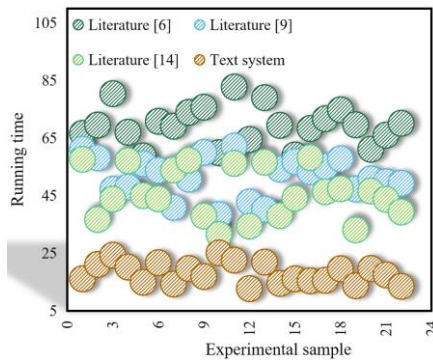


Figure 4: Running time of different privacy protection methods for data sets in other systems.

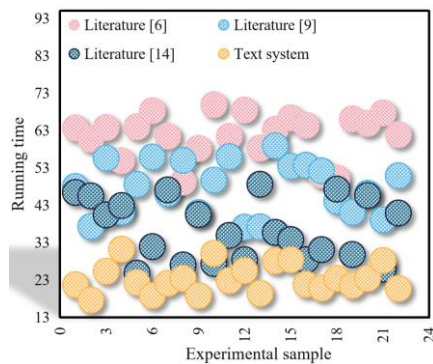


Figure 5: Statistical analysis results of privacy protection algorithms At runtime in different systems.

Through the above experimental analysis, to further verify the protection effect of the system built in this paper on workers' privacy, this experiment will select the literature [14] to compare with this system. The following experimental results are obtained by comparing the original data on different datasets and the performance after adding privacy, as shown in Figure 6 - Figure 7.

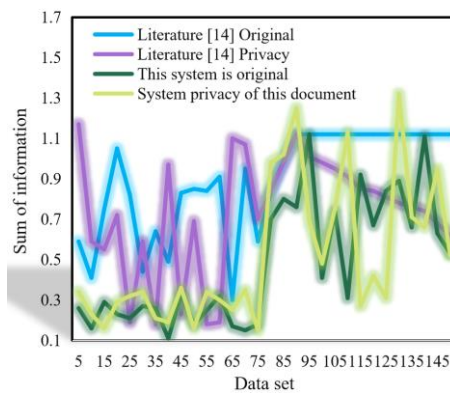


Figure 6: Comparison of the sum of information on different data sets.

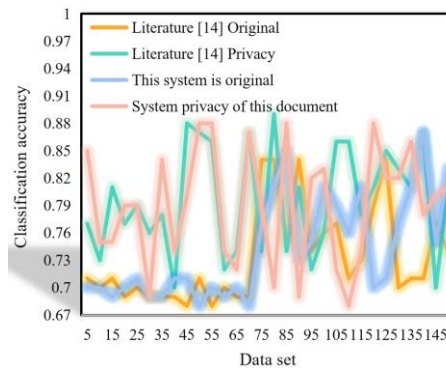


Figure 7: Comparison of classification accuracy on different data sets.

It can be seen from Figure 6 that after privacy is added, the sum of the information amount of the selected feature subset is smaller than the sum of the information amount of the selected feature subset without privacy protection, which indicates that the system in this paper can reduce the disclosure of privacy to a certain extent. The feature's privacy is protected because the amount of feature information chosen is relatively small. Figure 7 shows that the feature subset selected by the system in this paper has almost no significant change in classification, indicating that the selected features are valuable. The classification accuracy will not change too much because the features chosen still come from the original group after adding privacy. Still, the amount of information contained in the selected features is smaller than that of the features without privacy protection to protect the confidentiality of the features.

5 CONCLUSIONS

Workers' privacy rights are the specialization of privacy rights in labor relations, constituting an essential part of workers' fundamental human rights. Protecting workers' privacy is an inevitable requirement of respecting human rights and social progress. In China, the foundation of the privacy protection system is rather weak; so far, there are no clear, specific, and operable legal provisions for protecting workers' privacy, which makes the violation of workers' privacy happen frequently, and the protection is often ineffective after being violated. Therefore, this paper further analyzes the legal system of protecting workers' health and privacy based on big data in the network information environment. The research shows that when the data set is 95, The classification accuracy rate of this system is 75%. After privacy protection is added, the classification accuracy rate of the feature subset selected by this system is 76%, with little change, showing that the chosen features are helpful. After adding privacy, the selected features still come from the original grouping, so the classification accuracy will not change much, which can protect the privacy of features.

Yuxia Gao, <https://orcid.org/0009-0002-7271-9359>

ACKNOWLEDGMENTS

Research on teaching reform and practice in universities of Henan province: Innovative research on research teaching and research model under the Internet background.

REFERENCES

- [1] Aho, B.; Duffield, R.: Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China, *Economy and Society*, 49(2), 2020, 187-212. <https://doi.org/10.1080/03085147.2019.1690275>
- [2] Bengio, Y.; Ippolito, D.; Janda, R.: Inherent Privacy Limitations of Decentralized Contact Tracing Apps, *Journal of the American Medical Informatics Association*, 28(1), 2021, 193-195. <https://doi.org/10.1093/jamia/ocaa153>
- [3] Bhavé, D. P.; Teo, L. H.; Dalal, R. S.: Privacy at Work: A Review and a Research Agenda for a Contested Terrain, *Journal of Management*, 46(1), 2020, 127-164. <https://doi.org/10.1177/0149206319878254>
- [4] Boyne, S. M.: Data Protection in the United States, *The American Journal of Comparative Law*, 66(suppl_1), 2018, 299-343. <https://doi.org/10.1093/ajcl/avy016>
- [5] Cho, H.; Ippolito, D.; Yu, Y. W.: Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-Offs, *ArXiv Preprint Arxiv*. 111(36), 2020, 20-54.
- [6] Clayton, E. W.; Evans, B. J.; Hazel, J. W.: The Law of Genetic Privacy: Applications, Implications, and Limitations, *Journal of Law and the Biosciences*, 6(1), 2019, 1-36. <https://doi.org/10.1093/jlb/lisz007>
- [7] De, Stefano V.: Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection, *Artificial Intelligence and Labour Protection* (May 16, 2018). *Comparative Labor Law & Policy Journal*, 41(1), 2019, 16-28.
- [8] Feng, Q.; He, D.; Zeadally, S.: A Survey on Privacy Protection in Blockchain System, *Journal of Network and Computer Applications*, 126(15), 2019, 45-58. <https://doi.org/10.1016/j.jnca.2018.10.020>
- [9] Jan, N.; Khan, S.: Energy-Efficient Source Location Privacy Protection for Network Lifetime Maximization Against Local Eavesdropper in Wireless Sensor Network (EeSP), *Transactions on Emerging Telecommunications Technologies*, 33(2), 2022, e3703-e3719. <https://doi.org/10.1002/ett.3703>
- [10] Ji, Y.; Zhang, J.; Ma, J.: BMPLS: Blockchain-Based Multi-Level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems, *Journal of medical systems*, 42(8), 2018, 1-13. <https://doi.org/10.1007/s10916-018-0998-2>
- [11] Jia, B.; Zhou, T.; Li, W.: A Blockchain-Based Location Privacy Protection Incentive Mechanism in Crowd Sensing Networks, *Sensors*, 18(11), 2018, 3894-3899. <https://doi.org/10.3390/s18113894>
- [12] Kitsiou, A.; Tzortzaki, E.; Kalloniatis, C.: Identifying Privacy Related Requirements for the Design of Self-Adaptive Privacy Protections Schemes in Social Networks, *Future Internet*, 13(2), 2021, 23-33. <https://doi.org/10.3390/fi13020023>
- [13] Kuang, L.; Wang, Y.; Zheng, X.: Using Location Semantics to Realize Personalized Road Network Location Privacy Protection, *EURASIP Journal on Wireless Communications and Networking*, 20(1), 2020, 1-16. <https://doi.org/10.1186/s13638-019-1618-7>
- [14] McGraw, D.; Mandl, K. D.: Privacy Protections to Encourage Use of Health-Relevant Digital Data in a Learning Health System, *NPJ Digital Medicine*, 4(1), 2021, 1-11. <https://doi.org/10.1038/s41746-020-00362-8>
- [15] Moore, W.; Frye, S.: Review of HIPAA, Part 1: History, Protected Health Information, and Privacy and Security Rules, *Journal of Nuclear Medicine Technology*, 47(4), 2019, 269-272. <https://doi.org/10.2967/jnmt.119.227819>
- [16] Namara, M.; Wilkinson, D.; Lowens, B. M.: Cross-Cultural Perspectives on EHealth Privacy in Africa, *IEEE Transactions on Network Science and Engineering*, 33(10), 2018, 1-11. <https://doi.org/10.1145/3283458.3283472>
- [17] Price, W. N.; Cohen, I. G.: Privacy in the Age of Medical Big Data, *Nature Medicine*, 25(1), 2019, 37-43. <https://doi.org/10.1038/s41591-018-0272-7>

- [18] Sharon, T.: Blind-Sided by Privacy? Digital Contact Tracing, the Apple/Google API and Big Tech's Newfound Role as Global Health Policy Makers, *Ethics and Information Technology*, 23(1), 2021, 45-57. <https://doi.org/10.1007/s10676-020-09547-x>
- [19] Van, Kolschooten H.; de, Ruijter A.: COVID-19 and privacy in the European Union: A legal perspective on contact tracing, *Contemporary Security Policy*, 41(3), 2020, 478-491. <https://doi.org/10.1080/13523260.2020.1771509>
- [20] Xiong, J.; Ma, R.; Chen, L.: A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT, *IEEE Transactions on Industrial Informatics*, 16(6), 2019, 4231-4241. <https://doi.org/10.1109/TII.2019.2948068>
- [21] Yazdinejad, A.; Parizi, R. M.; Dehghantanha, A.: Blockchain-Enabled Authentication Handover with Efficient Privacy Protection in SDN-Based 5G Networks, *IEEE Transactions on Network Science and Engineering*, 8(2), 2019, 1120-1132. <https://doi.org/10.1109/TNSE.2019.2937481>
- [22] Zuiderveen, Borgesius F. J.: Strengthening Legal Protection Against Discrimination by Algorithms and Artificial Intelligence, *The International Journal of Human Rights*, 24(10), 2020, 1572-1593. <https://doi.org/10.1080/13642987.2020.1743976>