

Protection of Personal Information of Workers under Algorithmic Monitoring

Runxin Huang^{1,a,*}

¹*East China University of Science and Technology, 130 Meilong Road, Xuhui District, Shanghai, China*

a. icecake531@163.com

**corresponding author*

Abstract: In the digital era, with the rapid development of big data and algorithmic monitoring technology, the protection of personal information of workers has become an increasingly prominent issue. While enterprises pursue efficient management and business development, they must balance the reasonable use and protection of workers' personal information. Starting from the scenario of enterprises conducting algorithmic monitoring on workers, this paper describes the current situation and development, as well as the personal information protection risks that workers may face. It proposes relevant opinions and analysis based on judicial practice and, finally, through discussing legislative principles, presents suggestions for the protection of workers' personal information under algorithmic monitoring. This paper hopes to contribute to the construction of a more fair, transparent, and privacy-respecting work environment and to create a safe and dignified workplace ecology for all workers.

Keywords: Algorithmic Monitoring, Workers, Personal Information Protection

1. Introduction

In the era of informatization, enterprise management has experienced richer development, and the scope of workplace has expanded continuously from offline to online, with workers' every move subject to ubiquitous electronic monitoring. The use of algorithmic monitoring can promote wiser decision-making, more effective property protection, and productivity enhancement. [1] Workplace intelligent monitoring relies on obtaining workers' personal information as a premise, processing this information as its purpose, and ensuring its accurate and efficient operation through continuous information acquisition. [2] In fact, technological advancements have made surveillance of workers more detailed, potentially leading to the collection of more personal information and sensitive data. Due to the relationship between management and being managed, the concept of personal information protection may not fully apply to the protection of workers' personal information. [3] This paper, based on the scenario of workers being "managed" by enterprises under algorithmic monitoring, analyzes the current situation and development of algorithmic monitoring, as well as the potential risks to the protection of workers' personal information in this specific scenario. It proposes relevant opinions and analysis based on judicial practice and, ultimately, discusses the principles in legislative construction to elucidate the conceptual framework for legislative construction of the protection of workers' personal information under algorithmic monitoring in China.

2. Problem Statement: Legal Risks of Protecting Workers' Personal Information under Algorithmic Monitoring

Currently, workers operate under the invisible web of algorithmic monitoring, where the availability of data may reshape workplace relationships, and an increasing number of work activities and products generate traceable digital footprints. The visibility of data increases the likelihood of workers being managed and controlled, [4] giving rise to numerous issues, including failures in the practice of informed consent rules and conflicts between managerial rights and the right to be informed. [5] In the contemporary digital and intelligent work environment, algorithmic monitoring, as an essential tool for enterprise management, brings about legal risks regarding the protection of workers' personal information. These risks mainly stem from three aspects: firstly, enterprises may excessively collect workers' personal information, violating relevant laws and regulations; secondly, workers may provide "weak consent" due to information asymmetry, which does not meet the legal requirement of explicit consent; finally, if enterprises fail to implement effective security measures, workers' personal information may be at risk of leakage or misuse. These legal risks may not only lead to administrative penalties and civil compensation for enterprises but also trigger labor disputes, disrupt labor relations, and even limit the innovation capabilities of enterprises.

With the continuous penetration of algorithmic monitoring technology, the boundaries between work and private life are increasingly blurred, and workers' lives are being reshaped, with monitoring ubiquitous in the workplace—electronic surveillance, personnel analysis, interface management, mechanization, and large-scale data capture leading to constantly increasing work intensity and pressure. [6] Workers face significant challenges in protecting their personal information.

3. Judicial Practices and Issues in Protecting Workers' Personal Information under Algorithmic Monitoring

With the widespread application of artificial intelligence technology, especially the increasing prevalence of algorithmic monitoring in labor management, the issue of protecting workers' personal information has become increasingly prominent. In practice, the number of relevant judicial cases has been increasing year by year, revealing the universality and complexity of this issue. [7]

3.1. Algorithmic Monitoring of Workers by Enterprises during the Work Process

3.1.1. Workers' "loyalty obligations" to enterprises under algorithmic monitoring during the work process

In the case of "Yang v. Shanghai Xiaoyu Information Technology Co., Ltd. Labor Contract Dispute," the court's ruling emphasized that workers should cooperate with the employer's requirements in specific situations, such as providing computer passwords, to meet work needs. Such cooperation is considered a manifestation of workers' loyalty obligations to the employer. However, can workers refuse to provide relevant information under non-work-related requests? It should be recognized that workers can refuse. Workers' loyalty obligations to the employer are limited, and such obligations are confined to the reasonable scope within the work domain. When the employer's requests involve workers' personal privacy and are not directly related to work, workers have the right to refuse these requests.

3.1.2. The management function of “monitoring” in the workplace and the employer’s duty to inform

The forms of algorithmic monitoring in the workplace are diverse, for example, companies install “SuperEye” software on all work computers for monitoring purposes. In the case of “Xiu v. Haiyang City Rong Plastic Packaging Co., Ltd. Privacy Dispute,” the court deemed that the company’s installation of computer monitoring software is a legal act of self-management, aimed at more effectively supervising and managing work rather than infringing on workers’ personal privacy. This indicates that work computers are primarily used to complete tasks assigned by the company, and their use space is open to the company, which holds managerial rights. However, when implementing algorithmic monitoring, companies should clearly inform workers of relevant regulations and the scope of monitoring to balance the relationship between management needs and individual privacy rights.

3.1.3. Standards for Workers to Exercise the “Right to Refuse”

In the case of “Cheng v. Dantelaf Electronic Co., Ltd. Economic Compensation Dispute,” it was the refusal of the worker to return the laptop to the company for inspection without being informed of specific reasons that sparked discussions on whether workers can refuse enterprise algorithmic monitoring. The court proposed that “necessity” is an important criterion for judging whether workers can refuse enterprise management requests. At the same time, the court also emphasized respect for workers, stating that unreasonable pressure cannot be imposed on workers under the guise of “management.” This means that workers have the right to refuse unreasonable requests from enterprises within a reasonable scope to protect their personal information security.

Respect and understanding for workers are also considerations. The court noted that workers should be fully respected in their work; termination of labor contracts cannot be casually justified on this basis, and imposing unreasonable pressure on workers under the guise of “management” is considered to be “clearly beyond the reasonable protection of the company’s employment management rights under the law.” Respect between enterprises and workers should be mutual, not one-sided. Workers have the right to refuse unreasonable requests from enterprises without reasonable justification, thereby protecting their personal information security. The case also mentioned the “Worker’s Handbook,” which can stipulate relevant circumstances if necessary and reasonable.

Judicial practice regarding the protection of workers’ personal information under algorithmic monitoring demonstrates multidimensional considerations. When implementing algorithmic monitoring, enterprises not only need to consider the necessity of management but also fully respect the security of workers’ personal information, ensuring a balance of interests between both parties. When formulating and implementing monitoring policies, enterprises should clearly inform workers of relevant regulations to ensure the transparency and legality of monitoring behavior, thus fostering harmonious labor relations.

3.2. “Monitoring” of Workers during the Resignation Process and After Resignation

In modern workplace environments, it is common for workers to use computers provided by their employers for work. In this scenario, the ownership of the computer belongs to the company, so after a worker resigns, the company has the right to reclaim these computers. This practice can be understood from two perspectives.

Firstly, the company reclaims the computers out of consideration for protecting business information and maintaining information security. Workers may store a large amount of work-related information on the computers, including the company’s trade secrets. Therefore, reclaiming the

computers to ensure the security of this information is a manifestation of the company's legal rights. Secondly, the company's management and disposal rights over the provided computers are based on its ownership of property and the right to manage corporate affairs. Even after a worker resigns, the company still has the right to manage and dispose of work-related content on the computers.

However, the situation becomes complicated when it comes to whether workers can delete or handle information on the computers before resigning. In the case of "Li v. Biaoge Environmental Materials Co., Ltd. Labor Dispute," the worker formatted the company computer due to concerns about naval secrets and personal information, resulting in data loss. Since the worker failed to provide evidence supporting their actions, this act was considered serious negligence. The court ruled that storing personal information on the work computer was a personal act of the worker, and they should bear the consequences. Nevertheless, in reality, many workers still store personal information on work computers. There is inconsistency in the judicial practice regarding this practice. In the case of "Shi v. Heyi Management Consulting (Shanghai) Co., Ltd. Privacy Dispute," the court considered that if the information or files stored by the worker in the work computer "belong to personal privacy, are not intended to be disclosed to others, and are unrelated to others," then the company becoming aware of it is a result of the company's property management and the worker's improper storage behavior, rather than intentional infringement of the worker's privacy by the company.

In summary, workers who unilaterally handle information on work computers during the resignation process may face the risk of serious negligence. Regarding the personal information stored on work computers, there are differing views on who should bear the consequences: on one hand, some believe that workers should bear all consequences, while on the other hand, some believe it should be a joint responsibility of both the company and the worker. The author leans towards the latter, believing that companies should inform workers to inspect personal information on computers before and after resignation, as this is a basic respect for workers. At the same time, workers should also respect the rights of the company, ensuring the proper handling of personal information during the resignation process to avoid unnecessary trouble for both parties.

4. Principles and Guidelines for Addressing the Protection of Workers' Personal Information under Algorithmic Monitoring in China

Through the analysis of the current situation and judicial practices, we have found that, in the context of algorithmic monitoring, workers' personal information faces multiple challenges. These issues highlight the inadequacy of existing laws in protecting workers' personal information, especially in areas such as personality rights and privacy rights, where regulations are relatively broad and lack targeted protective measures. In order to more effectively protect workers' personal information, we can draw on international experience and propose a series of principles and guidelines based on China's actual situation.

As scholars have stated, "it is necessary to adjust laws to respond to new infringements on privacy rights brought about by social and technological changes." [8] Faced with the new challenges to privacy rights brought about by social and technological changes, adjustments to the law are particularly necessary. In today's increasingly widespread use of algorithmic monitoring, the protection of workers' personal information faces unprecedented challenges. As Moore and Hayes have described, "empowerment and disempowerment are typical characteristics of algorithmic monitoring in the workplace." [9] In order to establish a bridge of mutual connection and communication between enterprises and workers, which facilitates enterprise management while effectively protecting workers' personal information, the following principles and guidelines are particularly important.

4.1. Principle of Proportionality

The principle of proportionality has unique value in the protection of employees' personal information, providing procedures and standards for balancing the interests of both employers and employees and correcting the imbalance in the protection of employees' personal information. [10] From the practical perspective of workplace personal information protection, the principle of proportionality, namely balancing the legitimate business interests of employers and the privacy rights of employees, has always been the core principle and basic task of workplace personal information protection. [11] In order to safeguard the personal information rights and interests of workers, when managing and regulating employers, the spirit and requirements of the principle of proportionality should be followed, and principles of legitimacy, appropriateness, necessity, and balance should be applied. [12] Through the principle of proportionality, the extent of enterprise management of workers is limited, ensuring that the level of enterprise management of workers remains at the necessary minimum, in order to reconcile the management needs of the enterprise with the purpose of protecting the personal information of workers. When enterprises formulate their own management terms, attention should be paid to the application of the principle of proportionality, and terms that are practical should be formulated. The management methods of enterprises should be proportional to the effects achieved.

4.2. Principle of Informed Consent

The principle of informed consent requires enterprises to obtain explicit consent from workers before processing their personal information. This not only promotes transparency and accountability but also helps prevent potential privacy infringement issues. For example, to minimize the harm caused by weak consent, substantive review of labor regulations and contract contents involving the processing of workers' personal information should be conducted based on the principle of benefit consistency. [13] Before managing workers, enterprises should inform workers of: (1) the methods by which algorithmic monitoring or supervision will be conducted; (2) whether workers' work performance will be automatically monitored by a specific method of management employed by the enterprise; (3) if this method of management has a significant impact on workers. Workers should also have the right to request clarification from enterprises to better understand the enterprise's management methods and protect personal information.

The principle of informed consent emphasizes workers' right to choose. Enterprises should ensure that workers have the right to consent to or refuse the collection and use of personal information, especially in the collection of information required for non-critical job functions. Additionally, workers should have the right to revoke their consent at any time, and enterprises should provide convenient methods for doing so. Enterprises should implement appropriate technological and managerial measures to protect the security of workers' personal information and prevent unauthorized access, disclosure, modification, or deletion of information. This includes the application of encryption technology, the establishment of access control mechanisms, and regular security audits.

4.3. Principle of Occupational Differentiation

Based on the characteristics and needs of different workers, enterprises should adopt differentiated management methods. The principle of occupational differentiation means that enterprises manage differently according to the occupational needs of different workers. The two basic requirements of the principle of occupational differentiation are: distinguishing between workers covered by labor laws and other workers; setting different baseline rights for workers in different occupations. [14] The principle of occupational differentiation emphasizes the distinction between workers covered by

labor laws and other workers, which is crucial for ensuring the protection of the rights and interests of different categories of workers. For example, for workers who need to work in special environments (such as high-altitude, deep-sea, high-temperature environments, etc.), labor laws may have specific provisions, such as working hours, rest and vacation systems, to ensure the health and safety of these workers. When applying labor laws, enterprises should manage differentially based on the specific occupational characteristics of workers to ensure the effective implementation of legal provisions.

4.4. Principle of Necessity and Reasonableness

In the context of algorithmic monitoring, the handling of workers' personal information by enterprises should be based on the principles of reasonableness and necessity. Reasonableness means that enterprises should have a certain basis for management, especially legal basis. The law should play a role in coordinating the relationship between enterprises and workers, especially when workers are often in a weaker position. The law can restrict the specific forms of algorithmic monitoring through enumerative provisions. When enterprises carry out management, there should be reasonable and legitimate reasons. Necessity means that when enterprises carry out management, only necessary measures should be taken. In this case, personal information stored by workers in the workplace, such as personal data not necessary for performing work tasks, should not be obtained or used by enterprises. Necessity also lies in restricting algorithmic monitoring of workers to the workplace and work tasks, limiting monitoring outside the workplace, and prohibiting monitoring of workers after hours.

5. Conclusion

In the digital age, with the rapid development of big data and algorithmic monitoring technology, the protection of workers' personal information has become an increasingly prominent issue. While enterprises pursue efficient management and business development, they must balance the reasonable use and protection of workers' personal information. This paper, through analyzing relevant legal cases and principle guidelines, emphasizes the importance and urgency of protecting workers' personal information in the workplace. The protection of workers' personal information is a complex and multi-dimensional issue that requires concerted efforts from the government, enterprises, and society to gradually explore and improve. We look forward to building a fairer, more transparent, and privacy-respecting work environment, and creating a safe and dignified workplace ecosystem for all workers.

References

- [1] Aloisi, A., & Gramano, E. (2019). *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*. *Comparative Labor Law & Policy Journal*, 41, 95.
- [2] Xu, Q., & Wang, P. (2023). *On the Boundary of Workplace Intelligent Monitoring and Personal Information Protection of Workers*. *Hubei Social Sciences*, (03), 121-129. DOI:10.13660/j.cnki.42-1112/c.016061.
- [3] Hu, C. (2023). *Research on Personal Information Protection System for Workers*. *Journal of Anhui Business College of Vocational Technology*, 22(03), 58-62. DOI:10.13685/j.cnki.abc.000710.
- [4] Whittaker, X. (2018). *There Is Only One Thing in Life Worse Than Being Watched, and that Is not Being Watched: Digital Data Analytics and the Reorganisation of Newspaper Production*. In: Moore P., Upchurch M., Whittaker X. (eds) *Humans and Machines at Work. Dynamics of Virtual Work*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-58232-0_4
- [5] Abulimiti, A., & Zhao, Y. (2023). *Dilemma and Legal Countermeasures of Personal Information Protection of Workers under the Digital Economy*. *Business Economics*, (08), 25-27+187. DOI:10.19905/j.cnki.syjj1982.2023.08.048.

- [6] Moore, P. V., Upchurch, M., & Whittaker, X. (2018). *Humans and Machines at Work: Monitoring, Surveillance and Automation in Contemporary Capitalism*. In: Moore P., Upchurch M., Whittaker X. (eds) *Humans and Machines at Work. Dynamics of Virtual Work*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-58232-0_1
- [7] Liu, J., Zhong, D., & Li, Y. (2023). *Protection of Workers' Personal Information from the Perspective of Public Law—A Study on Safeguarding Workers' Right to Informed Consent*. *Journal of China Institute of Industrial Relations*, 37(05), 61-71.
- [8] Wilson, R. J., Belliveau, K. M., & Gray, L. E. (2017). *Busting the Black Box: Big Data, Employment and Privacy*. *Defense Counsel Journal*, 84(1).
- [9] Moore, S., & Hayes, L. (2018). *The Electronic Monitoring of Care Work—The Redefinition of Paid Working Time*. In: Moore, P., Upchurch, M., Whittaker, X. (eds) *Humans and Machines at Work. Dynamics of Virtual Work*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-58232-0_5
- [10] Zhang, Y. (2023). *Construction and Application of Proportionality Principle in Protection of Employees' Personal Information*. *Jiao Da Law Review*, (06), 158-172. DOI:10.19375/j.cnki.31-2075/d.2023.06.009.
- [11] Xie, Z. (2021). *The Legal Value, Basic Principles, and Legislative Path of Protecting Workers' Personal Information*. *Comparative Legal Studies*, (03), 25-39.
- [12] Li, W., & Li, H. (2023). *Application of Proportionality Principle in Protection of Workers' Personal Information in the Algorithmic Era*. *Journal of Southwest Petroleum University (Social Sciences Edition)*, 25(02), 81-87.
- [13] Wang, W. (2024). *On the Strength and Weakness Modes of the Rules of Informed Consent for Personal Information—With Discussion on Selection and Application in the Labor Relations Scenario*. *Journal of Southwest Petroleum University (Social Sciences Edition)*, 26(01), 82-94.
- [14] Pan, F. (2008). *On Legal Protection of Workers' Privacy: An Analytical Framework*. *Hebei Law Review*, (07), 108-114.