

Applying Impact Assessment to Protect Workers' Privacy in Intelligent Monitoring

Qi Wang^{1, *}, Zelin Tan²

¹ College of Economic Law, Shanghai University of Political Science and Law, Shanghai, China

² College of International Law, Shanghai University of Political Science and Law, Shanghai, China

*Corresponding Author: Qi Wang

ABSTRACT

In the context of the artificial intelligence era, the application of workplace intelligent monitoring technology improves management efficiency while posing a threat to workers' personal information security. This article analyzes the conflict between workers' personal information rights and the management rights of employers, and points out the inadequacies of existing laws in protecting workers' personal information. To address this challenge, the article proposes introducing Personal Information Protection Impact Assessment (PIPIA), aimed at improving transparency in information processing and workers' participation, while emphasizing the importance of the purpose limitation principle in monitoring activities. In response to the challenges in implementing PIPIA, the article suggests strategies such as refining assessment standards, improving labor laws, and strengthening the construction of supervisory departments, aiming to find a balance between intelligent monitoring and personal information protection.

KEYWORDS

Workplace Intelligent Monitoring; Workers' Personal Information Protection; Personal Information Protection Impact Assessment.

1. INTRODUCTION

Globally, employers have begun using advanced technologies such as smart wristbands, smart seat cushions, monitoring software, and body chips to conduct intelligent monitoring of workers. This has become a significant social phenomenon in the age of artificial intelligence. The Personal Information Protection Law provides a basic regulatory framework for workplace intelligent monitoring, but how to apply these regulations practically still requires in-depth research. Scholars have proposed various solutions, with some advocating from the perspective of consent and its limitations to seek a balance of interests; others suggest incorporating personal information protection into labor standards.[1] However, the Personal Information Protection Impact Assessment, as stipulated in the Personal Information Protection Law, has rarely been discussed. [2] The Personal Information Protection Impact Assessment is a preemptive compliance and risk evaluation process designed to assess the impact of personal information processing activities on individual rights and security risks. The nature of the Personal Information Protection Impact Assessment in addressing workplace intelligent monitoring issues has yet to be explored, so this article aims to investigate the application path of Personal Information Protection Impact Assessment in the context of intelligent monitoring in the workplace.

2. THE DILEMMA OF PROTECTING WORKERS' PERSONAL INFORMATION IN THE CONTEXT OF WORKPLACE INTELLIGENT MONITORING

SECTION HEADINGS

The section headings are in boldface capital and lowercase letters. Second level headings are typed as part of the succeeding paragraph (like the subsection heading of this paragraph).

2.1. The Conflict between Workers' Personal Information Rights and Employers' Management Rights

In the modern workplace environment, the application of intelligent monitoring technology has become an essential tool for companies to enhance efficiency and ensure security. However, its implementation often involves the continuous collection and analysis of employees' personal information. As the principal entity responsible for management, employers use this technology to optimize operational efficiency, while employees, though subject to management, should also enjoy the right to their personal information, which is crucial to safeguarding individual dignity. The legitimacy of employers using intelligent monitoring is grounded in law. On one hand, according to labor regulations, employers have the right to manage workers, including setting work plans, company rules, and determining the workers' job content, methods, time, and location. [3] Additionally, Article 8 of the Labor Contract Law stipulates that workers are obligated to disclose matters related to their labor contract to the employer, allowing companies to collect information related to the labor contract. These managerial rights provide a legitimate basis for employers to use workplace intelligent monitoring.

In the context of increasingly developed internet technology, workplace intelligent monitoring can prevent the leakage of trade secrets through moderate surveillance of employees' behavior, and record behavioral data as evidence for legal protection and accountability. [4] Due to the specific nature of the employer-employee relationship, workers do need to give up certain rights in the workplace. [5] However, it is crucial not to confuse the priority of rights: even employers with managerial rights must respect workers' personal dignity. Therefore, employers must respect the dignity of workers and ensure their personal dignity is not infringed upon while providing labor.[6]

2.2. Main Risks Faced by Workers' Personal Information

2.2.1. Alienation of the Informed Consent Principle in Employers' Handling of Workers' Personal Information.

In handling workers' personal information, the principle of informed consent faces practical challenges. According to Article 13, Paragraph 1 of the Personal Information Protection Law, obtaining personal consent is the primary legal basis for processing personal information. However, in the employer-employee relationship, workers, due to their relative disadvantage in terms of information access, economic resources, and technical capabilities, as well as their subordination to and dependency on the employer, often struggle to fully implement the informed consent principle. The nature of the labor relationship means that workers must comply with the employer's arrangements regarding work time, location, content, and method, which exacerbates the difficulty in protecting personal information. The variability of personal information and the complexity of processing methods, coupled with workers potentially lacking the time, energy, or expertise to fully understand the company's privacy policies, lead to insufficient awareness of the risks of personal information misuse.

In daily work, workers may be unaware of the processing of their personal information and are unable to effectively supervise or control it. This situation makes it difficult for workers to be "fully informed," thus undermining their autonomy and right to choose regarding personal information

protection. Additionally, in today's labor market, workers often default to accepting employers' monitoring measures due to the excessive collection of personal information by intelligent monitoring technologies, particularly in the face of fierce market competition. Workers, in an effort to maintain job stability, are typically reluctant to negotiate or dispute personal information protection with their employers. In some cases, workers might even voluntarily disclose personal information to enhance their competitiveness. For example, the application of facial recognition technology, which should be strictly regulated in daily life, is seldom contested by workers when used by employers for attendance management. Even in judicial decisions, courts frequently accept facial recognition records as evidence for attendance without fully examining their legitimacy or necessity. This reflects the workers' vulnerable position in labor relations, making it difficult to implement the informed consent principle in the protection of their personal information.[7]

2.2.2. Workers' Passive Position in Intelligent Monitoring Management

In the current labor environment, workers generally lack understanding of the specific content of intelligent monitoring systems and the depth of information collection, leading them to passively accept the management measures based on such monitoring. First, employers typically implement workplace intelligent monitoring to collect and process workers' personal information based on the necessity of human resource management, without requiring prior informed consent from the workers. This legal exemption allows employers to maintain a level of secrecy in their monitoring operations, reinforcing their managerial position and subtly pressuring workers to remain highly alert during work hours and scenarios, in order to fulfill their loyalty and diligence obligations.

Secondly, as technology advances rapidly and intelligent monitoring methods diversify in the market, the complexity of monitoring products and the algorithmic "black box" problem further increase the opacity of how workers' personal information is collected and processed. Although employers claim to implement intelligent management and protect workers' rights, they may inadvertently collect personal information excessively in ways that are not easily noticeable to the workers. Additionally, because employers often lack awareness of how to protect workers' personal information, improper handling or negligence in safeguarding such information may lead to risks of information leakage, infringing on workers' rights.

2.2.3. The Increased Risk of Manipulation of Workers Due to Workplace Intelligent Monitoring

Here, the theory of information fusion is important to mention. This theory suggests that when personal information from different sources is integrated, it can reveal more comprehensive and accurate personal characteristics than a single information source. In the digital work environment, this risk of information fusion is particularly prominent, as technological tools and platforms make it extremely easy to collect and integrate information. Moreover, due to the nature of the labor relationship, employers collect and process a more diverse and comprehensive range of workers' personal information throughout the entire labor contract period. By integrating and analyzing this data, employers can easily create a comprehensive personality profile of a worker, making them extraordinarily transparent to their employer. Additionally, intelligent monitoring systems rely on sophisticated algorithms to collect personal information and perform deep data mining and analysis to implement automated decision-making processes. The design of these algorithms helps employers increase labor efficiency while simultaneously exploiting the workforce. A typical example is in the food delivery industry, where optimized algorithms constantly reduce delivery time, thereby increasing the pressure on delivery personnel. Furthermore, employers' reliance on intelligent monitoring to issue automated decision-making instructions means that in case of disputes, employers are likely to attribute responsibility to the algorithms, making workers the manipulated subjects of intelligent monitoring.

2.3. Existing Legal Protection Mechanisms: Inadequacies and Challenges

From the perspective of current laws, China lacks specific protection for workers' personal information. In labor law, the current legislation focuses more on protecting the material interests of workers, and the Labor Contract Law's Article 8, which serves as the legal basis for employers to collect and process workers' personal information, is only a general provision and does not provide detailed regulations on the specific scope of information workers must disclose to employers. [8] Additionally, in the Personal Information Protection Law, there is a lack of targeted treatment for workers' personal information. For instance, in the area of automated decision-making, Article 24, Paragraph 2 of the Personal Information Protection Law primarily protects consumers, with the content and applicable scenarios differing significantly from those for workers. This misalignment means that measures designed for consumer protection may not effectively apply to the processing of workers' personal information.

Furthermore, the protection of workers' personal rights in China mainly comes into play after an infringement occurs. This post-violation remedy system presents two problems. First, when determining whether a worker's personal information rights have been infringed, it often requires balancing the employer's managerial functions, especially when the management process inevitably involves personal information processing. In judicial practice, the legal evaluation of workplace intelligent monitoring is sometimes lenient, with the legality of monitoring often based merely on the legitimacy of its managerial purpose, without sufficiently examining the democratic nature of the monitoring policy-making process, its public disclosure, and the appropriateness and proportionality of its implementation. This approach may overlook the comprehensive and rational evaluation of the monitoring behavior, thus affecting the full protection of workers' rights.

Second, when workers seek legal remedy through civil litigation, they often find themselves in an unfavorable position. Compared to employers, workers have limited economic resources and face an information asymmetry in terms of personnel management. Additionally, the time and financial costs associated with litigation can be a significant burden for workers. More importantly, the infringement of personal information by employers does not always result in immediate and obvious damage, and even when damage occurs, its exact amount is difficult to quantify. The difficulty in obtaining legal redress may, in turn, encourage employers to risk violations, creating an unfavorable situation for the protection of workers' rights.

3. THE ADVANTAGES OF INTRODUCING PERSONAL INFORMATION PROTECTION IMPACT ASSESSMENT (PIPIA) IN WORKPLACE INTELLIGENT MONITORING

3.1. Advantages Compared to Rights-Based Protection Approaches

In the context of intelligent monitoring, personal information protection faces unprecedented challenges, and traditional rights-based protection approaches are often insufficient in addressing these challenges. [9] The core of Rights-Based Approaches (RBA) is to grant information subjects a series of rights, relying on the "notice-consent" mechanism and compensation for infringement as safeguards. PIPIA, through risk identification, assessment, prioritization, and minimizing, monitoring, and controlling the probability or impact of adverse events, enables more refined and dynamic management of personal information protection.

First, PIPIA is more effective in responding to the risks posed by intelligent monitoring. By assessing the risks associated with personal information processing activities, PIPIA can identify potential risk points and implement corresponding risk mitigation measures, such as strengthening data encryption and restricting data access rights, thus reducing the risk of personal information misuse at the source. Second, PIPIA emphasizes risk prevention rather than damage compensation, which is more in line

with the need for personal information protection in the context of intelligent monitoring. Through preemptive risk assessments and preventive measures, PIPIA enables intervention before damage occurs, effectively preventing or mitigating the damage. In intelligent monitoring, the reasonable use of personal information plays an important role in social governance and economic development, and PIPIA, as a risk-based approach, offers a more reasonable and effective path for personal information protection.

3.2. Advantages Compared to Traditional Risk Regulation

In the digital age, the ubiquity and complexity of personal information processing activities exceed the capacity of traditional government regulatory models. Traditional regulatory approaches face limitations in terms of knowledge and resources, restricting their regulatory effectiveness. Therefore, shifting the responsibility for risk assessment to those who have significant advantages in information, technology, and operational efficiency—namely, the personal information processors (i.e., employers)—is a more reasonable and efficient choice. For employers, implementing Personal Information Protection Impact Assessment (PIPIA) is a concrete manifestation of the government's push to strengthen self-management and self-improvement of personal information protection measures.[10]

PIPIA requires employers to assess potential risks before using intelligent monitoring technology to process workers' personal information, ensuring that the monitoring activities do not infringe upon workers' privacy rights and personal information rights. In this way, employers can demonstrate their responsibility for personal information protection while complying with laws and regulations, thus establishing trust with workers. Additionally, the implementation of PIPIA brings several benefits to employers. It not only helps employers avoid legal risks arising from the improper handling of personal information but also improves organizational data governance capabilities by optimizing data processing workflows, which can provide a competitive advantage in a highly competitive market. Furthermore, through active communication with workers, employers can better understand their concerns and needs, thereby improving management strategies, increasing employee satisfaction, and fostering loyalty.

3.3. Enhanced Transparency in Information Processing and Increased Worker Participation

Transparency and participation are two key elements of Personal Information Protection Impact Assessment (PIPIA) that play a crucial role in employers' handling of workers' personal information.

First, improving transparency means that when employers conduct intelligent monitoring, they must disclose the purpose, methods, scope, and processing procedures of workers' personal information. This transparency requires employers to provide full information to workers, ensuring that workers clearly understand how their personal information is collected, used, stored, and protected. By providing easily understandable privacy policies and monitoring notices, employers can build trust with workers regarding their personal information processing activities. Transparency also involves continuous communication and updates about data processing activities so that workers are kept informed of any changes.

Second, worker participation is another core aspect of PIPIA. Employers should encourage and allow workers to participate in the development and assessment of monitoring policies. This participation helps employers identify and address potential issues in the monitoring process, thereby improving the effectiveness and acceptability of the monitoring measures. In the digital age, workers have increasingly high expectations regarding personal information protection. By implementing PIPIA, employers demonstrate respect for and protection of workers' rights.

3.4. An Important Tool for Implementing the Purpose Limitation Principle

The purpose limitation principle is a critical guiding principle for assessing the legitimacy and rationality of employers' implementation of workplace intelligent monitoring. However, principles alone are insufficient; they require corresponding institutional mechanisms to ensure effective implementation. The Personal Information Protection Impact Assessment (PIPIA) is an important tool for implementing the purpose limitation principle. By conducting PIPIA, employers can better understand and apply the purpose limitation principle. PIPIA requires employers to clearly define the specific purposes of monitoring before designing and implementing monitoring systems and assess the legitimacy and necessity of these purposes.

The implementation of PIPIA also helps employers evaluate and select monitoring technologies and measures that have the least impact on workers' privacy. For example, technologies that do not involve biometric data or tracking trajectories can be chosen, thereby minimizing the potential risks to workers' personal information rights while still achieving the monitoring objectives. Through the in-depth analysis and evaluation of PIPIA, employers can better balance management efficiency and the protection of workers' personal information.

4. IMPROVEMENT STRATEGIES TO ADDRESS THE ISSUES OF INTRODUCING PERSONAL INFORMATION PROTECTION IMPACT ASSESSMENT

4.1. Refining the Scope and Standards of Personal Information Protection Impact Assessment

In refining the scope and standards of Personal Information Protection Impact Assessment, a series of meticulous measures should be taken to ensure that the evaluation is both comprehensive and specific, while considering the characteristics of different scales and industries. Guidelines for evaluating different types of personal information should emphasize security in identity verification, ensuring that proper encryption measures are taken during transmission and storage to prevent unauthorized access.

Additionally, attention should be given to the unique needs of small and micro enterprises. For such businesses with limited resources, simplified assessment templates can be designed to reduce unnecessary administrative burdens. At the same time, online tutorials and tools can be provided to help them understand and apply the evaluation guidelines. Personal Information Protection Impact Assessment must be more precise and efficient, while also taking into account the specificity of different types of personal information and the practical situations of employers of varying sizes, thereby promoting a scientific and standardized approach to personal information protection.

4.2. Strengthening the Construction of Supervisory Departments for Workers' Personal Information

Strengthening the construction of supervisory departments for workers' personal information is a necessary measure for implementing the Personal Information Protection Law (PIPIA) in protecting workers' personal information. It is also a crucial means to enhance employers' internal motivation for personal information protection evaluations. Currently, China has not concentrated the supervisory responsibilities for personal information protection into a single department. According to Article 60 of the Personal Information Protection Law, the national cyberspace administration is responsible for coordinating the overall supervision, while other relevant departments are required to carry out their duties within their respective scopes.

Given the professional nature of personal information protection, traditional labor departments face limitations in technical regulation. Therefore, it is necessary to establish specialized personal information protection agencies within both central and local human resources and social security departments to ensure inter-departmental coordination and collaboration. Looking forward, the regulatory responsibility for personal information protection evaluations will likely be shared by the labor department and the cyberspace administration. To ensure comprehensive coverage of personal information protection in the labor sector and to address violations at different levels in a timely and effective manner, a clear division of labor and collaborative mechanism needs to be established. For violations involving fewer people or lighter infractions, labor inspection agencies can conduct preliminary investigations and address them. For more complex cases involving larger numbers of individuals or more serious violations, personal information protection agencies established by the human resources and social security departments should intervene and handle the cases.

5. SUMMARY

In the shadow of intelligent monitoring, the path to protecting workers' personal information, although fraught with challenges, is not without solutions. Through an in-depth analysis of the dilemmas of personal information protection under workplace intelligent monitoring, we reveal the subtle balance between workers' personal information rights and employers' management rights, as well as the inadequacies of existing legal protection mechanisms. Introducing the Personal Information Protection Impact Assessment (PIPIA) as a solution not only enhances the transparency of information processing and workers' participation but also serves as an important tool for implementing the purpose limitation principle, offering forward-looking risk management for the protection of workers' personal information. However, the implementation of PIPIA faces challenges, including its broad applicability, insufficient internal motivation, and incompatibility with labor laws. To address these issues, we propose refining assessment standards, improving related labor laws, and strengthening the construction of supervisory departments to build a balanced bridge between intelligent monitoring and personal information protection. In the future, we anticipate a harmonious interplay between law and technology, ensuring that workers' personal information remains secure even under the bright light of intelligent monitoring.

REFERENCES

- [1] Wenfang Wu (2022). The Application and Limitation of Consent in Employees' Personal Information Processing. *China Legal Science*, vol. 40, no. 1, pp. 221–240.
- [2] Qian Wang (2022). Personal Information Protection as a Labor Standard. *Peking University Law Journal*, vol. 34, no. 1, pp. 183–200.
- [3] Zhu Xiao (2021). Theoretical Interpretation and Systematic Construction of the Identification Standard for Labor Relationship Subordination. *Law Science*, no. 2, pp. 160–176.
- [4] Qiangsheng Xu & Pingping Wang (2023). On the Boundary Between Workplace Intelligent Monitoring and Employees' Personal Information Protection. *Hubei Social Sciences*, no. 3, pp. 121–129.
- [5] Xizhin Wang (2021). The State's Obligation to Protect Personal Information and Its Implementation. *China Legal Science*, vol. 39, no. 1, pp. 45–63.
- [6] Zhenxing Zhang (2021). The Labor Law Approach to Employee Personal Information Protection under the Civil Code. *Journal of Xi'an Jiaotong University (Social Sciences Edition)*, vol. 41, no. 6, pp. 146–158.
- [7] Qian Wang (2022). Personal Information Protection as a Labor Standard. *Peking University Law Journal*, vol. 34, no. 1, pp. 183–200.
- [8] Qian Wan (2011). Restrictions on Employers' Right to Know in the Recruitment Stage: Also on the Interpretation and Application of the Second Half of Article 8 of the Labor Contract Law. *Social Law Review*, vol. 5, no. 00, pp. 85–104.
- [9] Tao Zhang (2022). Exploring the Dimension of Risk Control in Personal Information Protection. *Law Science*, no. 6, pp. 57–71.

- [10] Quan Liu (2022). On Personal Information Protection Impact Assessment: Centered on Articles 55 and 56 of the Personal Information Protection Law. *Journal of Shanghai Jiao Tong University (Philosophy and Social Sciences)*, vol. 30, no. 5, pp. 39–50.