

职场监控下的劳动者个人信息权益保护

郭雅妮

上海政法学院国际法学院, 上海

收稿日期: 2025年6月2日; 录用日期: 2025年7月2日; 发布日期: 2025年7月9日

摘要

随着数字化技术的快速发展, 职场监控手段日益多样化, 包括视频监控、网络活动跟踪、算法监控与大数据分析等, 这些技术在提高管理效率和保护企业资产的同时, 也对劳动者隐私权和个人信息权益构成了潜在威胁。法律保护现状方面, 虽然我国《民法典》和《个人信息保护法》强化了个人信息权益保护, 但实践中仍存在问题。尤其在劳动关系中, 劳动者与用人单位的地位不平等, 导致劳动者在个人信息保护方面处于弱势, 维权成本高、难度大。域外经验借鉴中, 欧盟的《通用数据保护条例》(GDPR)及其配套意见书为平衡劳动监控与员工隐私权益提供了有益参照, 强调了数据处理的合法性、正当性与必要性, 并明确了雇主的新增责任, 特别是对处理合法性和信息收集范围的严格限制。由此, 我国应细化个人信息处理的具体规则, 明确监控界限, 强化劳动者知情同意的实质有效性, 确保信息处理的透明度; 同时, 应拓宽“员工”定义, 确保所有雇佣关系中的个人信息权益得到保护; 并且, 建立高效、低成本的维权机制, 加强劳动监察与法律救济, 确保劳动者在面对职场监控时能够有效维护自身权益。通过这些措施, 实现职场监控与劳动者个人信息权益保护的平衡, 促进劳动关系的和谐稳定。

关键词

劳动者个人信息权益, 职场监控, 用人单位

The Protection of Laborers' Personal Information Rights under Workplace Monitoring

Yani Guo

School of International Law, Shanghai University of Political Science and Law, Shanghai

Received: Jun. 2nd, 2025; accepted: Jul. 2nd, 2025; published: Jul. 9th, 2025

Abstract

With the rapid development of digital technologies, workplace monitoring methods have become

文章引用: 郭雅妮. 职场监控下的劳动者个人信息权益保护[J]. 争议解决, 2025, 11(7): 55-63.

DOI: 10.12677/ds.2025.117215

increasingly diversified, including video surveillance, network activity tracking, algorithmic monitoring, and big data analysis. While these technologies improve management efficiency and protect corporate assets, they also pose potential threats to laborers' right to privacy and personal information rights. In terms of the current status of legal protection, although China's "Civil Code" and "Personal Information Protection Law" have strengthened the protection of personal information rights, some practical issues remain. Especially in labor relations, the unequal status between laborers and employers has put laborers in a disadvantaged position in personal information protection, with high costs and difficulties in safeguarding their rights. In drawing on extraterritorial experience, the European Union's "General Data Protection Regulation" (GDPR) and its supporting opinions provide a useful reference for balancing labor monitoring and employees' privacy rights. They emphasize the legality, legitimacy, and necessity of data processing, clarify the new responsibilities of employers, and particularly impose strict restrictions on the legality of processing and the scope of information collection. Therefore, China should refine the specific rules for personal information processing, clarify the boundaries of monitoring, strengthen the substantive validity of laborers' informed consent, and ensure the transparency of information processing. Meanwhile, the definition of "employee" should be broadened to ensure the protection of personal information rights in all employment relationships. Additionally, an efficient and low-cost rights protection mechanism should be established, and labor supervision and legal remedies should be strengthened to ensure that laborers can effectively safeguard their rights in the face of workplace monitoring. Through these measures, a balance between workplace monitoring and the protection of laborers' personal information rights can be achieved, promoting harmonious and stable labor relations.

Keywords

Laborers' Personal Information Rights, Workplace Monitoring, Employing Units

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 职场监控问题与劳动者个人信息权益

(一) 数字化时代的职场监控

在数字化时代, 职场监控已成为企业管理中不可或缺的一部分。随着科技的发展, 监控手段从传统的物理监控演变为更为先进的数字监控技术, 数字监控也由最初的保障工作场所安全的作用转向了更多元化的作用, 比如保证员工的工作效率。与此同时, 它们也对劳动者的个人信息权益带来了前所未有的挑战。

如今日新月异的职场监控模式大致可以表现为视频监控、网络活动跟踪以及算法监控和大数据分析。

视频监控原本通常用于保障工作场所的安全, 防止盗窃和暴力事件的发生, 主要是通过摄像头对 workplaces 进行实时监控。但如今传统的视频监控系统已逐渐被智能化的高清摄像头所取代, 这些智能化的高清摄像头不仅具备基本的录像功能, 还能够通过先进的算法进行图像分析和模式识别。这些设备能够实现更多功能, 比如人脸识别, 系统能够自动识别和区分不同的个体, 有助于追踪特定人员的行为模式或确保只有授权人员进入特定区域。

网络活动跟踪是指用人单位监控员工的上网行为, 包括对员工的电子邮件、电话通话和网络活动进行监控, 防止信息泄露和不当行为, 因此也会便于用人单位评估员工的工作态度与效率。除此之外, 用人单位可能还会监视他们访问的网站、在线搜索记录和社交媒体活动, 以评估员工的在线行为是否与工

作相关。这通常可以通过以下技术手段实现：比如监控员工的网络流量，记录员工访问的网站、下载的内容以及上传的信息，或者对员工的网络搜索、电子邮件和即时通讯内容进行关键词扫描，以识别潜在的敏感或不当行为。

算法监控与大数据分析则是一种新兴的综合性的监控形式。通过分析员工的电脑操作记录、网络浏览习惯、工作产出数据等，算法能够评估员工的工作表现、行为模式甚至预测离职倾向，情感状态。比如，通过分析员工的工作数据，如完成任务的速度和质量，可以评估其工作表现；利用算法识别员工的行为模式，可以预测其工作习惯和潜在的工作效率问题；通过分析员工的网络行为和通讯记录，可以预测可能的信息安全风险或不当行为。比如 2022 年就有媒体报道，某互联网公司安装了行为感知系统，可对员工在单位网络内的网站访问记录进行分析，其中包括员工访问招聘网站的时长、频次等，用以做离职倾向分析¹。

尽管这些监控手段在一定程度上有助于企业实现其管理目标，但它们也引发了对劳动者隐私权的担忧。职场监控的目的应当是与工作需求直接相关且合理的。然而，智能监控对于劳动者个人信息处理的范围更广、程度更深、冒犯性更强、隐蔽性更高[1]，这就使监控的实施往往超出了合理的范围，涉及到了劳动者的个人生活领域。

(二) 劳动者个人信息权益与用人单位权益

1、劳动者个人信息权益的概念框架

个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等²。一般来说，一项信息是否构成个人信息，关键看该项信息是否具有“识别性”。“个人信息”这一法律概念的核心内涵在于“能够单独或者与其他信息结合识别自然人个人身份”[2]。《个人信息保护法》第四条第二款规定，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等³。

相比于一般自然人的个人信息权益，劳动者个人信息权益更为特殊，因为其限定于相对固定的时间和场所，而这样的时间和场所介于公共与私人空间之间[3]。个人信息保护法所调整的信息处理者与个人之间的关系，本质上是一种因信息不对称产生的不平等关系，而劳动关系的从属性特征更强化了这种不平等的程度[4]。在职场中的各个阶段，用人单位均会接触到大量的员工个人信息，与此同时，用人单位对这些个人信息的处理也紧密融入了整个用工管理周期。因此，劳动者个人信息权益，应包括对个人信息的知情权、决定权、查询权、复制权、更正权、转移权、删除权、要求解释权等。这些权利是劳动者人格尊严与个人自由的体现，也是其在数字时代工作环境中应当享有的基本人权之一。

2、员工的个人信息受保护权与用人单位知情权的冲突

在《民法典》和《个人信息保护法》的框架下，法律强调了个人信息处理的合法性、正当性与必要性原则，自然人的个人信息权益得到了法律保护。然而，在职场这一特定场景中，劳动者与用人单位之间固有的管理与被管理关系，使得员工个人信息权益的保护面临更大挑战。

一般意义上知情权是一种自然人专属权利权利[5]。但是用人单位作为能够以自己名义进行法律活动的法人也可以享有知情权。根据《劳动合同法》第八条规定，为了确保合同的有效履行，用人单位有权获取与劳动合同直接相关的基本情况，劳动者有义务如实提供⁴。这一规定赋予了用人单位一定的知情权，

¹《企业“监控”应恪守法律边界》，光明网 2022 年 2 月 23 日，<https://m.gmw.cn/baijia/2022-02/23/35537576.html>。

²《中华人民共和国民法典》第 1034 第 2 款。

³《中华人民共和国个人信息保护法》第 4 条第 2 款。

⁴《中华人民共和国劳动合同法》。

旨在维护企业的合法权益,确保招聘的适宜性和工作的顺利进行。然而,与一般知情权的权利主体不同,该权利主体处于强势地位,且义务主体对其存在较强的人身依附性[6]。用人单位对劳动者有一定的管理权,这导致用人单位知情权的行使与员工个人信息权益保护之间存在微妙的界限。“与劳动合同直接相关”的限度往往存在主观解读的空间,从而引发双方对个人信息范围的争议。例如,用人单位可能认为了解员工的社交账号有助于评估其社交能力与团队融入度,而员工则可能视之为个人隐私的侵犯。因此,如何合理界定知情权的边界,避免过度收集个人信息,就成为了关键问题。

2. 职场监控下对于劳动者个人权益的保护现状与困境

(一) 法律体系中的相关规范

1、法律规范分析

我国现行规范框架起初未对劳动者的个人信息保护权设立专门规定,主要依据民法中关于隐私权的一般规范解决相关纠纷。

2021年《民法典》的通过标志着隐私权和个人信息权益保护的强化,尤其在《人格权编》中详细规制了隐私权,并在《侵权责任编》中提及了特定情境如医疗情境下的保密责任。尽管《民法典》为隐私权提供了更全面的保护框架,包括确认自然人的隐私权、隐私的定义及确立个人信息中私密信息的处理规则,但在实际操作中,隐私与个人信息的界限依然模糊,特别是工作场所监控等情境下,员工隐私和个人信息的保护依然面临很大挑战。

同年出台的《个人信息保护法》为劳动关系中的个人信息处理提供了特定合法性基础,允许在一定条件下豁免个人同意,但这为用人单位滥用提供了可能,特别是在界定“必需”处理个人信息的标准上存在较大解释空间。加之劳动关系中双方地位不平等,个人同意往往非真正自愿,且大规模收集信息时单独同意的效率问题,使得个人信息保护路径在保护雇员隐私权方面存在局限性。因此,虽然法律规定相较于之前有所进步,但仍需进一步细化和完善相关解释规则及保护措施,以确保劳动者隐私权得到有效保障。

我国劳动关系立法传统上侧重于保护劳动者的物质性权益,如薪资、工作条件等,而对精神性权益,包括人格尊严和隐私权等保护不足。《劳动法》和《劳动合同法》中虽有原则性提及保护劳动者权利,但实际上对精神性权益的具体保护规定较为有限,尤其是隐私权方面,主要通过限制用人单位知情权来间接保护,规定用人单位仅能了解与劳动合同直接相关的基本信息。然而,对于“与劳动合同直接相关”的界定、劳动者未主动披露信息的法律责任、以及哪些具体信息属于应当披露的范围等问题,现有法律法规并未提供清晰界定,导致实际操作中存在较大解释空间和地域性差异,亟需更细致和统一的规范来填补这一空白。

2、算法监控的规制

应当建立更透明化的算法监控机制。用人单位在实施算法监控前,应以通俗易懂的语言向劳动者披露算法的数据收集范围、决策影响维度等。并且明确提示,算法监控仅能收集与工作直接相关的必要数据,禁止采集与工作无关的个人信息(如员工非工作时间的社交媒体言论)。例如客服行业算法监控只能记录与客户沟通的通话时长、关键词匹配度,不得获取员工私人通话内容。同时还可以强化数据安全保障:要求用人单位对算法监控收集的数据实施分级保护,采用加密存储+访问权限最小化双重保护,比如规定最多只能允许3名工作人员查看所收集到的数据,且行为轨迹数据定期删除(如超过6个月的计算机操作记录自动清除)。还可建立数据泄露应急响应机制,发生重大数据泄露时(如超1000条员工信息泄露),需在72小时内通知监管部门和受影响劳动者。

3、法律保护的基本原则

劳动者个人信息保护应遵循合法、公正、必要和透明等一般原则，同时确立比例原则为核心原则，以平衡雇主合法利益和雇员隐私权利[7]。要解决职场监控下劳动者个人信息保护的问题，最关键就是要看用人单位和劳动者双方如何确立界限，确保监控是适当行为，使工作场所的电子监控在道德合理的基础上成为进行高效合理企业管理的有效手段[8]。这就要求在涉及个人信息的任何处理活动中，用人单位必须确保其行为在法律框架内进行，处理过程公平公正，并且只在达成合法目的所需的最有限范围内进行，同时整个处理流程需对劳动者保持高度透明。这些原则共同确保了信息处理活动的正当性与合理性。而比例原则强调，在追求雇主的合法管理利益与保护雇员隐私权利之间，必须寻求一个恰当的平衡点。这意味着用人单位在采取任何监控或信息处理措施时，不仅要考虑其措施的合法性与必要性，还必须评估该措施对雇员隐私权益的影响程度，确保所采取的措施与其追求的管理目标相称，避免过度干预，从而在保护雇员个人信息权益与维护企业运营效率之间达到和谐稳定的平衡状态。

由于劳动关系的特殊性，知情同意原则的适用应严格限制。在原则上，雇员同意不能单独作为雇主处理个人信息的合法性基础[7]。因此，重要的是超越形式上的同意，深入探究劳动者给予同意的背景、条件及是否真正出于自愿。这要求用人单位在获取同意时，确保劳动者充分理解信息处理的目的、范围和可能后果，确保同意过程的自由、充分且无压迫感，以此作为个人信息处理的补充合法性验证，进一步加固个人信息保护的屏障。

(二) 职场监控环境下劳动者个人信息权益保护的挑战

1、信息不对称

在职场监控的实施中，信息不对称现象尤为显著。雇主作为监控系统的设置者和数据的最终接收方，拥有对监控技术的绝对控制权和信息处理的主导优势。相比之下，劳动者则处于相对弱势地位，难以充分了解个人信息的处理详情[4]。劳动者不仅对监控技术的运作原理缺乏深入了解，更难以全面知晓个人信息被收集、处理的范围与目的。这种信息的不对等导致劳动者在维护自身个人信息权益时显得力不从心，难以有效参与到关乎自己隐私权益的决策过程中。

除此之外，劳动者与用人单位之间的信息不对称还导致用人单位在实施监控措施时常常超越了必要且合理的限度。比如首先，监控范围的过度扩张表现为用人单位对员工的监控不再局限于工作时间内和工作地点上的行为，而是延伸至员工的私人通讯、社交媒体活动乃至家庭生活领域。其次，监控内容往往超出确保工作任务完成所需的合理范畴，涉及到了员工的个人习惯乃至情感状态。再者，即便是针对工作相关的信息收集，一些用人单位采用的监控手段也可能过于严厉或复杂，比如监控邮件与聊天记录等。这些做法已经严重侵害了劳动者的个人信息权益。

2、算法决策的不透明

在智能监控系统中，自动化监控与算法分析的应用日益广泛，它们能够基于海量数据快速做出人员评估、绩效考核等决策。然而，自动化监控与算法分析可能产生难以解释的决策结果，劳动者难以对于影响其职业发展的信息处理逻辑和结果提出质疑[9]。劳动者对自身数据的处理方式、评价标准及最终决策依据缺乏必要的认知和参与。这种不透明性不仅剥夺了劳动者对于自身信息使用的知情权和参与权，也可能因算法偏见而造成不公平待遇，进一步损害了劳动者的合法权益。

算法偏见，源于数据收集的偏差、算法设计者的主观预设或训练样本的局限性，可能导致系统性地低估或高估某些群体的表现，从而在无形中放大不平等[10]。劳动者可能因为算法模型未能充分考虑其独特性而受到不利影响，却又难以通过常规渠道提出异议或申诉，因为缺乏透明度的算法决策过程难以提供足够的反驳依据。比如，2021年亚马逊一位员工由于一天内去6次卫生间被算法捕捉而被开除，但实际原因是她患有“肠易激综合症”，所以上班的时候会频繁上厕所。尽管这名女员工提供了“病历”的相

关证明,但是亚马逊公司经理称其提供证明的时间太晚,因此仍被解雇⁵。

3、救济渠道的限制

劳动法律关系区别于民事法律关系的根本,在于其蕴含的人身、财产和组织上的从属性特征。劳动关系中,劳动者在一定程度上需服从用人单位的指挥管理,这种从属性决定了劳动者在职场中的相对弱势地位。由此,劳动者在面对个人信息权益受到侵犯时,寻求法律救济面临着更高的成本和难度。比如熊某、武汉汇生伟业贸易有限公司劳动争议案中,用人单位坚持要求该监控 24 小时打开,而熊某主张其在 8 小时工作时间以外仍需在此范围内住宿活动,由于公司明显侵犯了劳动者的基本隐私权而被迫提出离职。但法院认为,熊某对公司客厅安装摄像头的情况是知情的,熊某也未举证证明公司将其监控获得的视频资料随意公开或泄漏给他人,公司出于管理需要在该办事处的客厅安装摄像头的行为并不必然构成对员工隐私权的侵犯⁶。

由此可看出,对于试图维权的劳动者来说,一方面,证据采集成为一大障碍。职场监控环境下的个人信息权益侵犯往往隐蔽且复杂,劳动者很难独立收集到充分且有效的证据,证明侵权行为的存在及其造成的损害。另一方面,高昂的经济成本、时间成本及可能的就业机会成本,使得许多劳动者在权衡利弊后选择沉默,放弃维权。这种现象不仅损害了劳动者的个人权益,也纵容了违法侵权行为。

尽管《侵权责任法》第十五条规定了侵权行为的民事责任承担方式。然而,在劳动关系背景下,仅依靠《侵权责任法》难以有效应对由劳动纠纷引发的深层次问题,如时间成本的累积、经济负担的加重,以及劳动者在维权过程中可能面临的职业发展的阻碍。这些问题的复杂性要求法律救济机制必须更加贴近劳动关系的实际情况,提供更加具体、可行且能有效降低劳动者维权门槛的解决方案。

3. 职场监控下对于劳动者个人权益保护体系的完善

(一) 域外经验借鉴

1、欧盟立法经验

2016 年生效、2018 年实施的《通用数据保护条例》(GDPR),替代了旧有的《数据保护指令》,升级了数据保护规则并强化了个人数据权益。为适应 GDPR 新框架,第 29 条工作组于 2017 年发布了《关于工作中数据处理的第 2/2017 号意见》,重申并扩展了先前关于职场数据处理的立场,明确了 GDPR 对雇主新增的责任,特别是在处理合法性、适用范围和具体监控场景应用上,特别强调了平衡劳动监控与员工隐私权益的重要性。

该意见书不仅限缩了“同意”作为工作数据处理的法律基础,还拓宽了“员工”定义,覆盖所有雇佣关系,并通过实例分析提供了实践指导。GDPR 将区分“无争议同意”与“明示同意”作为保护个人数据的重要条款提出,但“同意”细分是否必要则是一个值得商榷的话题。GDPR 通过将同意进行细分增加了对个人数据保护的门槛,但这种繁琐的程序究竟在多大程度上有助于提升个人数据的保护程度引发了理论界和实务界的讨论^[11]。

GDPR 与第 29 条工作组的意见共同构建了欧盟电子监控的统一规范框架,为雇主提供了操作基准,同时要求成员国雇主还需遵循本国数据隐私法及特定劳动监控条例。欧盟各国普遍建立了数据保护法律体系,并逐步将之适用于劳动环境,部分国家如比利时和芬兰,通过专项协议或立法,如比利时的第 81 号国家集体协议和芬兰的《工作中的隐私保护法》,明确界定了监控的合法基础、类型及程序,直接规制企业电子监控活动,保护员工隐私。在这些特定立法之外的多数成员国,则主要通过司法判决来确立电子监控中员工隐私权的保护规则,体现了 GDPR 原则与各国具体实践的结合与适应。

⁵ 亚马逊被起诉!原因竟是女员工一天上六次厕所遭开除,《CNMO 手机中国》2021 年 8 月 23 日。

⁶ 熊某、武汉汇生伟业贸易有限公司劳动争议案,湖北省武汉市中级人民法院(2020)鄂 01 民终 3509 号民事判决书。

2、域外经验启示

首先，欧洲联盟《通用数据保护条例》(GDPR)及其第 29 条工作组发布的相关意见书明确指出了在劳动监控领域内，寻求企业管理效率与员工个人隐私权益之间的平衡是至关重要的。这一平衡策略要求我们既要确保企业的合法管理需求得以满足，以维护工作场所的安全与效率，同时也要充分尊重并保护员工的个人隐私，避免监控措施过度侵犯个人生活空间，造成不必要的心理压力或权益损害。为此，我国在完善相关法律法规时，应当细化监控措施的合法性、正当性与必要性标准，确保每一项监控措施都有明确的法律依据，且其实施范围和程度与管理目的紧密相关，避免任何不必要的信息收集与处理。

其次，鉴于我国地域广阔、经济社会发展不平衡的现实情况，在国家层面，应当有一套全面而系统的个人信息保护法规，为全国范围内的个人信息处理活动设定统一的基本原则和标准。与此同时，鼓励和支持地方政府根据本地的经济发展水平、行业特色和社会文化背景，制定更加具体、可操作的实施细则或通过司法判例积累，不断丰富和完善个人信息保护体系。

另外，在界定个人信息保护法规的适用范围时，应当拓宽“员工”概念的内涵与外延，确保无论是全职、兼职、远程工作者，还是通过平台经济等新兴业态就业的劳动者，都能在个人信息保护的法律框架内获得应有的权益保障。

(二) 劳动者个人信息权益保护的完善

1、明确界定劳动场合的监控界限

明确监控界限是平衡企业管理和个人隐私保护的关键。这要求法律应详细规定何种类型的监控措施是被允许的，以及在何种条件下实施。比如，监控应当限于工作相关区域和时段，避免侵入员工的私人空间和非工作时间。同时，监控内容也应局限于与工作绩效、安全或合规性直接相关的信息，避免过度收集与工作无关的个人信息。

另外，智能监控应具有明确、合理且与劳动直接相关的目的。这意味着，首先用人单位在部署智能监控系统前，应详细阐述监控的具体意图，如提高生产效率、保障工作场所安全等。明确目的不仅能减少误解和猜疑，还便于监管机构和劳动者本人对监控活动的合法性和必要性进行评判。其次，在设计监控方案时，应综合考量各种因素，确保所采取的监控级别适度，既能达成管理目标，又不至于对劳动者的尊严和隐私造成不必要伤害。

最后，使用监控在实现管理目标的同时，最大限度减少对劳动者个人权益的侵犯。这不仅涉及监控的范围和频率，还涉及到数据收集后的处理与存储。例如，仅收集实现管理目的所必需的最少信息，对收集到的数据实施严格的访问控制和加密保护，以及定期审查和清理不再需要的数据，都是落实这一原则的具体举措。

2、确保劳动者持续性的知情同意权

劳动者在工作场所也应享有合理的隐私期待利益与隐私空间，这是保护其人格尊严的必要条件^[12]。劳动者的知情同意权的核心在于保障劳动者拥有对自己个人信息被收集和处理的自主控制权。这意味着在任何监控措施实施之前，用人单位必须遵循透明化原则，对监控活动进行全面而详细的说明。知情同意规则在实践中效果并不显著，并未完全实现立法者保护个人信息的目的^[13]。为了确保劳动者能够基于充分信息做出同意与否的决定，用人单位需要主动提供信息，还需使劳动者有足够的时间和资源去理解这些信息，并提出疑问。并且在征询同意的过程中，避免任何形式的诱导、误导或胁迫，确保同意的自愿性和真实性。

值得注意的是，知情同意并非一次性的行为，而是一个持续的过程。随着监控技术和管理需求的变化，用人单位应及时向劳动者更新信息，重新征得同意，尤其是在监控范围、目的或方式有所调整时。此外，还应设立简便的撤销同意机制，使劳动者在任何时候都能基于个人意愿改变其决定，而不用担心

遭受不利后果。

3、扩大劳动者的救济渠道

首要任务是强化劳动监察体系，使之成为捍卫劳动者隐私权益的坚固防线。这意味着必须将劳动者个人信息权益的保护明确列为劳动监察部门的职能之一。除此之外具体而言，监察部门应主动采取定期检查与随机抽查相结合的方式，审核用人单位是否遵循了相关法律法规关于个人信息收集、存储、使用的严格规定。此外，应当鼓励劳动者在遭遇或疑似遭遇侵权时，能够第一时间向劳动监察部门举报。监察部门可以设立专门的隐私保护热线或在线举报平台，保证举报渠道的畅通无阻，并对每一起投诉进行认真调查，对确有违法行为的单位及时予以纠正，必要时采取行政处罚，形成强大的威慑力。

其次，在司法实践中，应当简化证据提交与认定程序，以减轻劳动者在维权过程中面临的举证负担。这一措施目的在于克服当前法律救济体系中存在的障碍，即劳动者在遭遇个人信息被非法监控或滥用时，往往因缺乏有效证据或举证过程繁杂而难以维护自身权益。第一，对于涉及技术复杂性的证据，如加密数据、算法分析结果等，监管机构应提供技术支持，协助劳动者获得证据，使之成为可被法庭采纳的形式。第二，减轻举证负担的核心在于降低劳动者证明侵权行为的难度。传统法律框架下，“谁主张，谁举证”的原则往往令处于信息弱势地位的劳动者承受巨大压力。因此，应考虑引入“举证责任倒置”机制，在特定情况下，如当劳动者初步证明个人信息可能被非法监控时，转而要求用人单位承担不存在侵权行为的举证责任。这样，不仅能有效抑制用人单位潜在的违法行为，也能激励企业自我规范，采取更加透明和合规的监控措施。

4. 结论

职场监控技术的发展在提升企业管理效率的同时，也对劳动者个人信息权益构成系统性挑战。从现实来看，视频监控的智能化升级、网络活动跟踪的全面化覆盖、算法监控的自动化决策，正不断突破传统劳动权益保护的法律边界，而信息不对称、算法不透明、救济渠道有限等问题，进一步加剧了劳动者的弱势地位。

在法律层面，虽然我国《民法典》和《个人信息保护法》搭建起了个人信息保护的基本框架，但劳动关系所具有的从属性特征，使现有规则在实际适用过程中遭遇“同意形式化”“界限模糊化”“责任空心化”等难题。欧盟的《通用数据保护条例》(GDPR)通过细化数据处理的合法性基础、拓宽“员工”定义以及强化雇主的透明义务等举措，为平衡监控需求与隐私保护提供了有益借鉴。不过，我国还需结合本土劳动关系的特点，构建更具针对性的保护体系。

完善劳动者个人信息权益保护，需明确监控仅限工作时空及必要内容，智能监控需说明正当目的并控制数据收集与处理；算法监控应透明披露数据范围与决策逻辑，禁止采集无关信息，强化数据加密与泄露响应；确保劳动者知情同意的持续性与真实性，随监控变化更新同意并设撤销机制；强化劳动监察与司法救济，监察部门定期抽查并设举报平台，司法上简化证据程序、引入举证责任倒置。

职场监控与个人信息权益的平衡，本质上是效率与公平、管理秩序与人格尊严的价值调和。唯有通过法律规则的精细化设计、监管机制的创新性构建、企业责任的实质性落实，才能在数字时代实现劳动关系的和谐发展，让技术进步真正服务于人的尊严与自由。这不仅是法律制度完善的必然要求，更是数字文明时代劳动权益保护的应有之义。

参考文献

- [1] 梁栋. 数智化职场中劳动者个人信息保护的特性、价值与规则[C]//北京理工大学法学院,上海市法学会.《智慧法治》集刊 2024 年第 2 卷——“东方法学新锐”研究文集. 2024: 104-116.

<https://www.booksci.cn/article/118514.htm>

- [2] 张新宝. 《民法总则》个人信息保护条文研究[J]. 中外法学, 2019, 31(1): 54-75.
- [3] 田思路. 智能化劳动管理与劳动者隐私权的法律保护[J]. 湖湘论坛, 2019, 32(2): 16-27+2.
- [4] 田野. 职场智能监控下的劳动者个人信息保护——以目的原则为中心[J]. 中国法学, 2022(3): 102-118.
- [5] 张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
- [6] 丁芳. 用人单位知情权及其边界[J]. 金陵科技学院学报(社会科学版), 2017, 31(2): 71-75.
- [7] 谢增毅. 劳动者个人信息保护的法律价值、基本原则及立法路径[J]. 比较法研究, 2021(3): 25-39.
- [8] 王红雷. 工作场所电子监控的企业伦理分析[J]. 管理现代化, 2002(6): 59-61.
- [9] 汤晓莹. 算法技术带来的劳动者隐私风险及制度因应[J]. 中国人力资源开发, 2021, 38(8): 65-81.
- [10] 刘友华. 算法偏见及其规制路径研究[J]. 法学杂志, 2019, 40(6): 55-66.
- [11] 王雪乔. 论欧盟 GDPR 中个人数据保护与“同意”细分[J]. 政法论丛, 2019(4): 136-146.
- [12] 田野. 工作场所电子邮件监视与雇员隐私权保护[J]. 北京科技大学学报(社会科学版), 2008(1): 65-71.
- [13] 廖丽环. 个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分[J]. 法制与社会发展, 2022, 28(6): 156-180.