

数字时代劳动者隐私权保护的困境与路径研究

李昊玥

西南林业大学文法学院，云南 昆明

收稿日期：2025年7月7日；录用日期：2025年7月22日；发布日期：2025年8月25日

摘要

数字时代背景下，人工智能与物联网技术的深度应用使企业智能监控系统全面渗透劳动场景，导致劳动者隐私权面临系统性风险。当前我国劳动者隐私权保护存在立法体系碎片化、智能监控技术滥用、告知同意规则异化等问题，其根源在于劳动关系的从属性结构、技术发展带来的双重性挑战以及利益平衡机制的缺失。研究表明，应通过构建保护路径，完善相关立法体系，健全隐私权救济机制，重构告知同意规则，从而提升劳动者在信息处理中的参与度与选择权。该研究为在数字化治理背景下实现企业管理效率与劳动者权益保护的协调提供了制度参考。

关键词

数字时代，劳动者隐私权，保护困境，立法体系

Research on the Dilemma and Path of Protecting Workers' Privacy Rights in the Digital Era

Haoyue Li

School of Humanities and Law, Southwest Forestry University, Kunming Yunnan

Received: Jul. 7th, 2025; accepted: Jul. 22nd, 2025; published: Aug. 25th, 2025

Abstract

In the context of the digital era, the deep integration of artificial intelligence and the Internet of Things has enabled enterprise-level intelligent surveillance systems to extensively penetrate labor scenarios, which has posed systemic risks to workers' privacy rights. The protection of such rights in China has faced a series of challenges, including fragmented legislation, excessive use of surveillance technology, and the distortion of the informed consent mechanism. These problems have stemmed from

the inherent subordination in labor relations, the dual-edged nature of technological development, and the absence of effective interest-balancing mechanisms. This study has proposed a comprehensive protection path by improving the legislative system, enhancing the remedies for workers' privacy rights, and reconstructing the rules of informed consent to ensure workers' substantive voluntariness. The research has offered institutional references for balancing corporate management efficiency and the protection of individual rights in the digital age.

Keywords

Digital Era, Workers' Privacy Rights, Protection Dilemma, Legislative Framework

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. 引言

在数字技术迭代加速的当下，人工智能算法与物联网设备的深度融合正重塑着劳动管理范式。企业通过部署智能监控系统实现管理效能的指数级提升，管理模式在优化人力资源配置的同时，正引发劳动者隐私权的系统性风险。据中国信息通信研究院 2024 年调查显示，83.6% 的受访企业承认使用数字化监控手段，其中 47.2% 的系统具备生物特征识别功能，而劳动者对监控行为的知情同意率仅占 32.1%。这种技术赋能与管理异化的矛盾，将监控触角延伸至劳动者私人生活空间，导致工作场所与私人领域的界限彻底消融。

2. 数字时代劳动者隐私权保护存在的问题

(一) 立法保护体系的碎片化与适用性不足

我国劳动立法体系对劳动者隐私权的保护呈现明显的碎片化特征，尚未形成系统性规范。现行法律中仅在个别条款中涉及隐私保护，却缺乏明确的权利界定与救济路径。首先，立法内容分散且模糊。《劳动合同法》第 8 条仅规定用人单位有权了解劳动者“与劳动合同直接相关的基本情况”，但未明确“直接相关”的界定标准，亦未规定隐私保护的例外情形与救济途径[1]。这种模糊性导致司法实践中出现“同案不同判”现象。例如，在“某科技公司员工健康数据泄露案¹”中，法院认定企业收集体检信息属于履行劳动合同必要措施；而在“某物流企业定位追踪案²”中，持续追踪员工行踪却被认定为隐私侵权。

现有的劳动法律仅规定用人单位侮辱劳动者时需要承担行政责任或刑事处罚，这对于劳动者人格权的保护是远远不够的[2]。《民法典》与《个人信息保护法》构建的民事保护框架，在劳动关系中面临适用性不足的困境。个人信息与隐私不同，其关键在于能否识别特定人的信息，包括个人姓名、住址、医疗记录、出生日期和身份证明等；应当对个人信息进行类型化划分，对与个人隐私存在交叉的“个人敏感隐私信息”的保护层级要高于其他类型的个人信息[3]。现有法律未对劳动场景下的“个人敏感隐私信息”作出特殊保护规定，导致民事法律对劳动者隐私的保护层级与劳动关系的特殊性不匹配[4]。民法体系以“平等主体”为前提，而劳动关系中用人单位天然占据强势地位。现有法律未建立劳动场景下的隐私保护特殊规则，如未明确工作设备与私人设备的使用界限、下班后信息处理的合法性边界，导致“数字劳工”在非工作时间仍可能受算法监控，陷入“全天候隐私暴露”的困境。

¹宁夏回族自治区银川市中级人民法院(2021)宁 01 民终 2013 号。

²安徽省合肥市蜀山区人民法院(2021)皖 0104 民初 6463 号。

(二) 智能监控技术对劳动者隐私权的多维侵犯

随着人工智能广泛应用于工作场所,用人单位获取劳动者个人信息的能力得以强化,在人工智能技术深度渗透工作场景的当下,智能监控技术对劳动者隐私权的侵犯已突破传统边界,呈现出范围扩张与手段隐蔽的双重特征[5]。这种多维侵犯不仅重构了劳动管理场景,更将劳动者置于全天候、无死角的监控网络之中。

监控范围的无边界扩张构成了首要威胁。智能监控技术已突破物理空间与数字空间的界限,形成立体化数据采集体系。在物理空间层面,UWB 智能工牌结合 WiFi 探针技术,可实现劳动者行动轨迹的厘米级追踪,办公场所内的每一次位移都被转化为可分析的数据坐标。在数字空间维度,终端监控软件悄然捕获键盘输入、屏幕截图、文件传输等操作痕迹,元数据分析技术甚至能通过操作频率、窗口切换模式重构劳动者思维图谱。监控手段的隐蔽性与持续性加剧了隐私侵蚀的深度。技术实施的物理隐蔽性体现在微型摄像头、隐形麦克风等设备的无感部署,劳动者往往在毫不知情的状态下被纳入监控网络。企业要求员工在私人手机安装监控软件的行为,更将监控触角延伸至非工作时间,劳动者下班后的行踪轨迹、社交活动乃至睡眠数据都被纳入监控范畴。这种持续性监控不仅压缩了私人生活空间,更在劳动者心理层面投射出“全景敞视监狱”的阴影。

(三) 告知同意规则在劳动关系中的异化

在《个人信息保护法》的框架下,“告知-同意”规则被确立为个人信息处理的核心原则,其本质在于通过信息主体的知情选择,实现对个人信息的自主控制与人格尊严的维护。信息处理者在收集使用个人信息时告知信息主体并获得其同意,是信息主体对个人信息控制和支配的体现,因此这一规则的意义在于尊重信息主体在个人信息保护中的人格自由。然而,当这一规则嵌入劳动关系场域时,其制度初衷因劳资双方的结构性力量失衡而发生显著异化[6]。劳动者虽在形式上作出“自愿同意”的意思表示,但这种同意往往受制于劳动关系中的从属地位与经济依赖关系,难以体现真实的意志自由,本质上沦为资本逻辑下用工管理权规训的形式化仪式,导致个人信息自主控制的制度价值在劳动关系中被弱化。

从属性劳动关系消解了同意的实质自愿性。依据《民法典》第 1035 条,个人信息处理需以明确同意为前提,但劳动关系中用人单位与劳动者的管理从属性,使得这种“同意”丧失了平等对话的基础。在入职环节,企业往往通过格式合同将监控条款与劳动关系的建立强行绑定。这种“全有全无”的选择机制,实质是将监控授权异化为获取就业机会的准入门槛。劳动者若拒绝签署包含监控条款的劳动合同,等待他们的往往是“不予录用”的冰冷通知。

信息不对称加剧了知情同意的形式化困境。劳动者所具备的知识并不能对个人信息的收集使用乃至泄露的结果作出理性预期和判断,退一步说,在强势地位的用人单位面前,劳动者即便预见个人信息权益可能被侵犯,可能也会在权衡利弊之后服从安排。智能监控技术的复杂性远超普通劳动者认知范畴,而用人单位却利用技术优势构建信息壁垒[7]。劳动者虽“知情”监控存在,但未必真正理解监控范围与数据用途。企业采用的智能监控系统能实时分析聊天记录,却未向员工明示数据采集边界与算法逻辑,这种技术黑箱使劳动者的“同意”沦为对未知风险的盲目接受。更甚者,部分企业通过专业术语堆砌的隐私政策,将监控授权包装成“数字迷宫”,进一步剥夺劳动者的知情权。

3. 劳动者隐私权保护困境的成因分析

(一) 劳动关系的从属性本质

在劳动关系中,组织从属性与经济依附关系交织作用,共同构成劳动者隐私权益受限的深层结构性成因。依据《劳动合同法》第八条,用人单位享有了解与劳动合同直接相关情况的知情权,而这一管理权在数字技术加持下被无限放大。企业通过部署如“超级眼”等智能监控软件,将管理边界由工作场所

延伸至私人通信领域，甚至将如厕频次纳入考核体系。这种管理边界的模糊化，反映出用人单位在制度结构中的权力优势。对于依赖工资维持家庭生计的劳动者而言，拒绝接受监控条款往往意味着就业机会的丧失。在此背景下，技术工具成为组织规训的延伸，构建出一种近乎“全景敞视”的数据环境，使劳动者处于持续被观察的心理压力之下。然而，从属性并非仅止于管理实践层面的依附，更应在规范与理论层面厘清其限度与合法性。根据 Guy Davidov 的观点，从属性虽是劳动法合法结构的核心基础，但当其滑向不可制约的支配，就已越出法律所容许的正当范围。共和主义自由观进一步提出“非支配”原则，认为即便劳动者形式上同意接受管理，只要缺乏对退出机制与反制途径的制度保障，即可视为潜在支配状态。将此观点嵌入数字监控语境，意味着当前技术赋权型管理极易在制度性从属性的外衣下生成不对称控制逻辑。因此，应从“合理－必要－透明”三个维度对用人单位的监控行为进行审查，以防止从属性悄然滑向支配，维护劳动关系中的基本权利边界。

美国的多数州与联邦法院认为信息隐私权是各州宪法和联邦法院中规定的“自由权”中所包含的重要权利的一种。我国则认为隐私权作为一项具体的人格权，属于绝对权和支配权，具有对世效力[8]。他人应当在法律规定范围内，合理、合法地获取个人隐私，不得任意侵犯。在传统劳动关系中，人格从属性体现为对劳动者行为的时间、空间约束；而在智能监控时代，这种控制已渗透至认知与情感领域[9]。某科技公司采用的“数字画像”系统，通过分析员工邮件情绪词汇、会议发言语调，生成“工作投入度指数”，直接关联晋升考核。更具侵略性的是，企业利用可穿戴设备监测脑波活动，试图解码员工的“潜意识工作效率”。这种技术规训将劳动者异化为“被动嵌入数据治理体系”，其心理边界与主体意识受到持续侵蚀。

（二）技术发展的双重性挑战

人工智能技术深度融入人力资源管理后，彻底革新了用人单位对劳动者的管理维度。通过部署智能监控系统，企业得以构建起覆盖时间管理、社交媒体动态、通信记录、屏幕操作轨迹、网络检索行为及生物特征识别等多元场景的立体化监管网络，实现劳动者行为数据的全天候、无死角采集。该技术体系不仅可精准追踪员工邮件收发频次、网页浏览轨迹、文档编辑记录及软件使用模式等基础信息，更能依托机器学习算法对海量原始数据进行深度解析，从而挖掘出传统管理手段难以察觉的关联性规律与潜在风险特征。这些直接或间接获取的数据可以为以数据驱动为基础的人事管理决策提供指标，成为用人单位录用、考核和解雇员工的依据[10]。

数字技术的迭代升级为隐私侵权行为配备了更具隐蔽性与高效能的技术工具链。在物联网架构下，办公设备、生产工具、交通工具等均被转化为数据采集节点，形成覆盖工作场景的“数字触角”网络，实现对劳动者行为轨迹、操作习惯乃至生理特征的全时感知。这些技术应用常以“智能化管理”“流程优化”为名义，通过算法脱敏、分布式采集等技术手段掩盖数据滥用本质。更值得警惕的是，预测性监控技术的普及已突破传统侵权的时空界限，企业可基于历史数据构建行为模型，对员工潜在风险进行前置评估与干预，使隐私侵权呈现出从被动采集向主动预判、从显性干预向隐性规训的异化特征。

（三）利益平衡机制的缺失

在数字资本与劳动权益的博弈中，利益平衡机制的缺失成为劳动者隐私权保护的致命伤。这种失衡既体现为企业管理权的结构性扩张，又折射出社会协调机制的全面失效，最终在算法时代演变为系统性权利侵害。在资本逻辑驱动下，管理目的从保障生产安全转向全面控制劳动者。雇主的监视可能对劳动者产生精神压迫与心理影响，危及健全的人格，左右劳动者在精神压迫下所做的行为，从而形成劳资间的精神从属性关系。而大数据最核心的技术特征就是超强的收集、存储和及时、精确地处理数据的能力以及精准的预测能力，这些特征对隐私存在天然的侵犯性[11]。社会利益协调机制的失效形成治理真空。在法律层面衡量劳资双方的利益平衡，应当坚持价值判断问题的实体性论证规则，即在没有足够充分且

正当理由的情况下,不得主张限制民事主体的自由[12]。法律规定缺乏操作细则,导致企业自证门槛过低[13]。技术治理层面,智能监控设备准入制度缺失,市场充斥大量隐私保护不合规产品。平台经济领域尤为典型,外卖算法持续压缩配送时间,将交通风险转嫁给劳动者,而社会尚未建立风险共担机制。

当前“利益平衡”沦为抽象主张的关键在于缺乏制度化的分析框架。借鉴《欧盟通用数据保护条例》(GDPR)中提出的“合法利益评估三步法”(Legitimate Interest Assessment, LIA),可对企业数据行为进行正当性审查:首先,企业监控目的是否具有合法性与明确性;其次,监控手段是否为实现该目的的“最小必要”方式;最后,企业的管理利益是否超过了劳动者的个人隐私权益。这一框架可为中国构建劳动数据治理机制提供评判工具。此外,德国比例原则(Proportionality Principle)所倡导的“正当-适当-必要-最小侵害”四种判断路径,也可被用于劳动监控行为的合法性审查,从而为“平衡”劳动者隐私权与企业管理权提供可操作的评价准则,防止权利天秤失衡为企业所单方面操控。

4. 数字时代劳动者隐私权保护的路径重构

(一) 完善立法体系,明确权利边界

在数字技术深度渗透劳动场景的背景下,劳动者隐私权保护需以立法体系重构为基础,通过细化规范、明确权利义务边界,平衡企业管理需求与个人隐私权益。在《劳动合同法》中细化企业监控告知义务。若基于劳动合同的要求或是签署劳动合同的必要条件,企业应当告知劳动者拒绝接受可能产生的后果。针对企业智能化监控中的“形式告知”问题,法律需明确告知事项的具体范畴[14]。企业在实施监控或收集私密信息时,应以通俗语言告知劳动者:监控的法定依据、劳动合同约定或签约必要性;监控手段及对隐私的潜在影响;数据存储主体、保护措施;是否以自动化决策结果作为职位考核依据。通过细化告知义务,防止企业滥用监控权,保障劳动者知情权与选择权。在《劳动法》中增设劳动者隐私权保护条文,构建“权利-义务-救济”三位一体的规范体系。一方面,明确劳动者隐私权的内涵,将生物识别信息、数字轨迹等新型隐私形态纳入保护范围;另一方面,设定用人单位监控行为的合法性要件:目的需正当、手段需必要、程序需合法。可借鉴德国《联邦数据保护法》,要求企业引入智能监控前完成“数据保护影响评估”,并提交工会审议,从源头控制隐私风险。但需指出,该机制在我国现实中推行面临制度约束,如目前尚无工会参与企业数据治理的成熟渠道,且中小企业普遍缺乏评估能力,实施成本较高。因此,可考虑先在大型平台企业或公共部门试点,由主管部门引导形成标准化评估模型,逐步推广制度常态化,避免“一刀切”式立法带来的执行落差。细化《个人信息保护法》在劳动关系中的特别规则,针对劳动场景特殊性,构建“一般规定+特别规则”的二元适用机制。建立敏感信息处理的“双重同意”规则,用人单位处理劳动者健康数据、生物特征等敏感信息时,除书面同意外,需经劳动行政部门备案审查,明确告知同意豁免情形。立法体系完善既能为数字时代劳动隐私保护提供明确规范依据,也能通过权利边界的清晰界定,实现企业管理效率与劳动者人格权益的平衡。

(二) 健全劳动者隐私权的救济路径

针对我国劳动者隐私权保护执法主体缺位问题,我国尚未建立健全系统性的劳动者隐私权保护执法机构。在数据安全方面,尽管我国采纳了以国家网信部门为中心的集中模式,但其执法努力主要集中于国家数据安全,而非个人数据隐私权保护。可借鉴欧盟集中管理模式,在国家网信部门下设立专门数据保护局,统一制定劳动者隐私保护细则,并对侵犯隐私行为行使行政处罚权。但考虑到我国监管架构层级复杂,数据治理职能分散于网信、工信与人社等多部门之间,新设机构在编制、预算与立法授权层面面临现实困难。更具可行性的方案是在现有网信部门设立“劳动数据保护专员”制度,通过授权专员对重点企业进行抽查审计,辅以地方人社部门联动,形成可控、可评估的监管合力。同时,应警惕集中模式带来的执法资源过度集中风险,可通过数据合规第三方参与机制分担审查压力,降低治理成本。

为破解劳动者维权成本高、举证难的困境，可赋予工会代表劳动者提起集体诉讼的权利。工会作为劳动者维权机构而行动，有利于规范潜在的诸如集体停工、怠工等劳动者集体争议行动，协助处理劳资利益争议。比如，借鉴证券市场投服中心特别代表人诉讼模式，允许工会就批量隐私侵权事件发起诉讼，避免个体劳动者因弱势地位放弃维权；建立智能数据审计制度，由政府或第三方机构对企业算法进行合规审查，帮助工会提取侵权证据，减少就业歧视等隐蔽侵权行为；工会通过集体诉讼规范劳资争议处理流程，替代停工、怠工等激进维权方式，既降低劳动者维权成本，又优化企业合规管理环境[15]。

(三) 重构告知同意规则，保障劳动者实质自愿

在智能化劳动管理场景中，传统“告知-同意”规则因劳动关系从属性特征面临异化风险，劳动者“同意”常沦为形式化程序。劳动者与企业签订合约，可以提前约定好企业对于劳动者智能管理的界限、使用手段以及信息使用与监控的程度等等。重构告知同意规则需以“实质自愿”为核心，通过细化告知标准、规范同意效力等路径，破解职场隐私保护中的意思自治困境[16]。

具体化告知要件要从“形式披露”到“有效知情”。用人单位须以醒目方式呈现关键信息，禁止将监控条款隐藏于冗长隐私政策或使用极小字体，避免通过“埋雷式告知”变相剥夺劳动者知情权。例如，欧盟《透明度指南》明确要求核心条款需加粗显示，我国可借鉴此标准，规定监控目的、数据类型等信息必须在劳动合同附件或单独告知书中突出标注。监控实施前必须完成告知，紧急情况需在风险消除后补正；告知内容需涵盖数据存储主体、自动化决策规则等细节，杜绝“概括授权”现象。

规范同意效力要从“默认接受”到“实质自治”。针对劳动关系中“同意”的非自愿性，需确立四项原则：第一，自愿性排除强权干预；第二，特定性禁止概括同意；第三，明确性否定默认授权；第四，合理性限制同意边界。劳动者需以主动勾选、书面签字等方式明示同意，系统预设“同意”选项或沉默行为不得视为认可。但值得注意的是，“实质自愿”原则在高流动性岗位与平台经济场景下实施将面临企业合规成本与用工管理效率的权衡挑战。尤其是在算法驱动型考勤系统中，若完全排除数据授权绑定，可能导致企业管理机制失效。因此，应区分“高敏感信息”(如健康、定位、私域通讯)与“操作性数据”，对前者施以强监管、强告知，而对后者可设例外处理条款，避免因过度规范反向挤压合法数据处理空间。

5. 结论

本文揭示了数字劳动场景中劳动者隐私权保护的制度困境与技术挑战，论证了从立法、救济与规则层面重构保护体系的必要性，明确劳动者隐私权的新型保护范畴，通过细化企业告知义务与监控合法性要件，填补当前法律对劳动关系特殊性回应不足的缺口。救济机制的创新形成了覆盖侵权预防、争议解决、权利救济的全链条保障，希望能有效破解劳动者维权成本高与举证弱势的困境。告知同意规则的实质化重构，则通过将形式化的“同意”转化为劳动者真实意思自治，从根本上遏制算法管理权的过度扩张。数字时代的劳动者隐私权保护，本质是对技术治理与劳动伦理的重新定义。文章中提出的路径为司法实践提供了统一裁判标准，更希望推动了劳动法治从“形式平等”向“实质公平”的范式转型。未来需进一步探索智能监控技术的合规边界，如建立算法审计制度与隐私影响评估机制，在技术创新与人格尊严之间构建动态平衡的治理框架，为数字经济时代的劳动关系法治化提供理论支撑与制度方案。

参考文献

- [1] 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(5): 25-39.
- [2] 黄薇. 中华人民共和国民法典人格权编解读[M]. 北京: 中国法制出版社, 2020: 198.
- [3] 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.
- [4] 张新宝. 雇员在工作场所的隐私权保护与限制[J]. 现代法学, 1996(5): 4-14.

-
- [5] Ernst, E., *et al.* (2018) The Economics of Artificial Intelligence: Implications for the Future of Work. ILO, 1.
- [6] 常宇豪. 论信息主体的知情同意及其实现[J]. 财经法学, 2022(3): 80-95.
- [7] 张继红, 郑书康. 论劳动者个人信息处理的合法性基础[J]. 上海大学学报(社会科学版), 2022, 39(1): 1-17.
- [8] 阿丽塔·L·艾伦, 理查德·C·托克音顿. 美国隐私法学说、判例与立法[M]. 冯建妹, 石宏, 郝倩, 等, 译. 北京: 中国民主法制出版社, 2004: 102.
- [9] 程啸. 我国民法典对隐私权和个人信息的保护[N]. 人民法报, 2020-07-30(5).
- [10] Aloisi, A. and Gramano, E. (2019) Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context. *Comparative Labor Law and Policy Journal*, **41**, 95-121.
- [11] 张义德. 论资讯化时代中劳动行踪监视——雇主之劳务指挥权、设施管理权确保 vs. 劳工隐私权[J]. 中正大学法学集刊, 2018(59): 190.
- [12] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149.
- [13] 王轶. 民法价值判断问题的实体性论证规则——以中国民法学的学术实践为背景[J]. 中国社会科学, 2004(6): 104-116, 206.
- [14] European Union (2016) General Data Protection Regulation (GDPR).
- [15] 侯玲玲. 比较法视野下的劳动者集体争议行动之法律规制[J]. 法律科学, 2013, 31(4): 104-116.
- [16] 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.