

人工智能时代下劳动者隐私权保护的挑战与应对

王国旗

宁波大学马克思主义学院, 浙江 宁波

收稿日期: 2026年6月18日; 录用日期: 2026年6月30日; 发布日期: 2026年7月24日

摘要

人工智能技术正深刻重塑现有的劳动管理模式, 同时也对劳动者隐私权构成系统性威胁。电子监控的泛在化、敏感信息的过度采集以及社交媒体的渗透, 使劳动者在工作场所几乎丧失私人边界。保护劳动者隐私权不仅是维护人格尊严的底线要求, 也是矫正劳资关系权力不对等、防范技术异化的内在需要。然而, 现行法律框架在应对上述挑战时存在着明显滞后。本文从劳动者隐私权保护的必要性、挑战与应对三个维度展开分析, 提出通过完善立法、规范企业知情权、技术监管等多元路径, 构建人工智能时代劳动者隐私权的有效保护途径。

关键词

人工智能时代, 劳动者, 隐私权, 个人信息保护, 技术监管

Challenges and Countermeasures for the Protection of Laborers' Privacy Rights in the Era of Artificial Intelligence

Guoqi Wang

School of Marxism Studies, Ningbo University, Ningbo Zhejiang

Received: June 18, 2026; accepted: June 30, 2026; published: July 24, 2026

Abstract

Artificial intelligence (AI) technologies are profoundly reshaping the existing labor management models, while also posing systemic threats to laborers' privacy rights. The ubiquity of electronic

monitoring, the excessive collection of sensitive information, and the penetration of social media have left laborers with almost no private boundaries in the workplace. Protecting laborers' privacy rights is not only a bottom-line requirement for safeguarding human dignity, but also an inherent need to rectify the power imbalance in labor-capital relations and prevent technological alienation. However, the current legal framework is obviously lagging behind in addressing the aforementioned challenges. This paper conducts an analysis from three dimensions: the necessity of protecting laborers' privacy rights, the existing challenges, and the corresponding response strategies. It proposes to construct an effective protection approach for laborers' privacy rights in the AI era through multiple paths, including improving legislation, regulating enterprises' right to know, and strengthening technological regulation.

Keywords

The Era of Artificial Intelligence, Laborers, Privacy Rights, Personal Information Protection, Technological Regulation

Copyright © 2026 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

人工智能是依托算法与大数据,模拟、延伸人类感知、思考、决策能力,可自主完成复杂任务的技术科学体系[1]。在人工智能发展浪潮中,数字技术加速迭代,不仅革新了信息载体与运算模式,更从活动空间、联结机制、组织形态到行动主体,对整个社会体系进行了全方位重塑[2]。人工智能正以前所未有的深度介入劳动关系的各个环节,从招聘筛选、绩效评估到日常监督乃至解雇决策,算法与智能系统正在取代传统的人力管理方式。这一变革无疑提升了管理效率,却也使劳动者面临前所未有的隐私侵蚀风险。近年来,劳动者和用人单位因为隐私权侵犯引发的劳动争议屡次上报,如2020年“宁波一公司,摄像头装在办公室通道顶,员工沟通无果用塑料袋遮挡被开除”¹,到2023年“强制查看员工手机,不给就辞退”²,再到2026年“员工因离座9分钟,和同事说话4分钟,提前4分钟离开工位,定性为严重违纪被开除”³。其共同点都是劳动者认为自己的隐私权受到了伤害,工作场所的监控从“看得见的摄像头”演变为“无处不在的数据触手”,劳动者的每一次点击、每一次心率波动、每一次社交媒体浏览都可能被记录、分析并用于决策。问题的核心在于:当技术赋予用人单位前所未有的监控能力时,劳动者的隐私权还能否获得有效保护?现有法律框架是否足以应对人工智能发展带来的新挑战?这些问题不仅关涉个体劳动者的尊严与自由,更触及数字时代劳动关系的根本重构。本文将从必要性、挑战与应对三个维度系统分析劳动者隐私权保护问题,以期为制度完善提供参考。

2. 人工智能时代下劳动者隐私权保护的必要性

2.1. 维护劳动者人格尊严与自主性的底线要求

隐私权作为一项具体人格权,是指自然人享有的私人生活安宁与私人信息秘密依法受到保护,不被

¹参见《宁波一公司,摄像头装在办公室通道顶,员工沟通无果用塑料袋遮挡被开除,法院判了》

(https://zjnews.zjol.com.cn/zjnews/nbnews/202112/t20211206_23453748.shtml, 访问时间2026年6月15日)。

²参见《为找“内奸”查员工手机,不配合就辞退?》(<https://baijiahao.baidu.com/s?id=1762573126213220384&wfr=spider&for=pc>, 访问时间2026年6月15日)。

³参见《这样管理企业,得不偿失》(<https://www.peopleapp.com/column/30052380770-500007542872>, 访问时间2026年6月15日)。

他人非法侵扰、知悉、搜集、利用和公开的一种人格权[3]。根据《中华人民共和国民法典》(以下简称《民法典》)的规定,自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。在人工智能时代背景下,各类的智能装置由于和人类相当的思维体系和行为方式,在一定程度上具有侵犯公民隐私权的风险,也可以作为侵犯隐私权的主体[4]。在人工智能监控的全面渗透下,劳动者的一举一动都可能被数据化记录、量化评价,从工位上的坐姿、鼠标点击频率,到工作中的表情变化、语音语调,都可能被算法解读为工作态度与能力的评价依据。这种“全景敞视”式的监控,将劳动者的个体行为拆解为冰冷的数据,消解了劳动者作为“人”的主体性,使其沦为被算法管控的“数字客体”。保护劳动者的隐私权,本质上是维护劳动者的人格尊严,保障其在工作场景中仍能保有基本的行动自由与心理安宁,避免因过度监控陷入被监视的压迫感与不安全感。

2.2. 矫正劳动关系中权力不对等的内在需要

劳动关系天然存在用人单位与劳动者之间的地位差异,用人单位掌握着生产资料、技术资源与管理权限,而劳动者在就业市场中往往处于相对弱势的地位。人工智能技术推动劳动关系从传统的“劳动者-用人单位”二元结构,演变为“劳动者-用人单位-人工智能”的三元互动模式[5]。人工智能技术的应用进一步放大了这种权力不对等:企业拥有数据采集、存储、分析的技术控制权,而劳动者往往缺乏对数据用途、范围与去向的知情权,更难以拒绝企业提出的不合理监控与数据采集要求。部分企业以“用工管理需要”为名,通过格式条款要求劳动者概括授权同意所有数据采集行为,劳动者为获得就业机会往往只能被动接受,难以实现真正的“知情同意”。加强劳动者隐私权保护,能够通过制度设计约束企业的数据权力,平衡双方在数字劳动关系中的地位,矫正技术加持下的权力失衡问题。

2.3. 防范技术异化与算法风险的制度屏障

人工智能是一把双刃剑。在提升效率的同时,其自身也蕴含着异化的风险。技术本应是服务于人的工具,但在缺乏有效约束的情况下,技术可能反过来支配人。当算法成为事实上的“管理者”,劳动者的行为被不断调整以迎合系统的偏好,人的主体性便让位于算法的逻辑。这种异化风险在劳动领域表现得尤为突出。外卖骑手被系统精确计算配送时间,稍有延迟即遭罚款;客服人员被AI监控通话时长与话术合规性,任何偏离都可能影响绩效;程序员被记录代码行数与提交频率,创造力退化为计件劳动。在这些场景中,劳动者不再是技术的使用者,而成了技术规训的对象。更为隐蔽的是算法歧视风险。人工智能系统可能继承历史数据中的偏见,对特定性别、地域或年龄的劳动者进行隐性排斥。由于算法决策过程高度不透明,这类歧视极难被发现与举证。建立劳动者隐私权保护制度,正是为了在技术系统中嵌入人类的价值判断,这不是对技术发展的阻碍,而是确保技术始终服从于人本价值的制度屏障。

3. 人工智能时代下劳动者隐私权保护的挑战

3.1. 电子监控对劳动者个人隐私的侵犯

电子监控是当前企业管理中应用最广泛的人工智能技术手段,其对劳动者隐私的侵犯主要体现在监控范围的过度扩张与监控方式的隐蔽化两个方面。一方面,部分企业的电子监控突破了“工作必要”的原则,将监控范围延伸至劳动者的私人空间与休息时间:例如在员工工位安装无死角摄像头,监控劳动者的工作状态;通过办公软件记录劳动者的屏幕操作、键盘输入与网络浏览记录;通过定位设备追踪劳动者的行动轨迹,甚至在非工作时间仍对劳动者进行定位追踪。这种全天候、无死角的监控,模糊了工作与生活的边界,严重侵犯了劳动者的私人生活安宁权。另一方面,电子监控的方式愈发隐蔽,部分企业通过后台程序、隐藏摄像头等方式采集劳动者数据,劳动者往往并不知道自己正处于被监控状态,更

无法对监控行为进行监督与抗辩。此外，部分企业将监控数据与绩效考核直接挂钩，例如根据劳动者的在线时长、点击频率等数据进行量化考核，迫使劳动者在监控下长期处于高压状态，对劳动者的心理健康也造成了负面影响。

3.2. 数据过度采集对劳动者敏感信息的侵犯

在人工智能管理模式下，企业的数据采集已不再局限于劳动者的工作信息，而是延伸至大量敏感个人信息，而这些信息的采集与使用往往缺乏有效的规范约束。人脸、指纹、声纹等生物特征信息作为《中华人民共和国个人信息保护法》(后文简称《个人信息保护法》)界定的“敏感个人信息”⁴，具有唯一性、不可替代性。企业通过人脸打卡、指纹考勤等方式采集劳动者的生物识别信息，通过健康申报、体检报告获取劳动者的健康数据，通过情绪识别系统分析劳动者的表情、语音等生理数据，甚至通过员工入职背景调查、社交账号关联等方式获取劳动者的家庭信息、社交关系与私人言论。这些敏感信息一旦被不当使用或泄露，将对劳动者的人身权益造成严重威胁：生物识别信息无法像密码一样修改，一旦泄露可能被用于身份冒用；健康数据的泄露可能导致劳动者遭受就业歧视；私人言论与社交动态的不当使用，则可能成为企业解雇劳动者的理由。同时，劳动者对这些敏感信息的采集往往缺乏有效的知情与同意机制，企业通常通过格式条款要求劳动者一次性授权所有数据的采集与使用，劳动者无法对不同类型的信息采集进行区分同意，也无法知晓数据的存储期限、使用范围与安全保护措施，个人信息权益难以得到有效保障。

3.3. 社交媒体监视对劳动者私生活安宁的侵犯

随着社交媒体的普及，部分企业开始将监控范围延伸至劳动者的私人社交领域，通过公开社交媒体平台、第三方监控工具，收集劳动者的网络言论、社交动态、兴趣爱好等信息，并将其与职业评价挂钩。即使劳动者努力在生活和在工作之间保持明确的界限，但在社交媒体中，他们的个人信息依然会很容易地被雇主基于管理名义的需要所获知，并被用来作为入职、奖惩与辞退的依据[6]。例如部分企业通过监控员工的朋友圈、微博、抖音等平台内容，判断员工的思想动态、工作态度，甚至将员工在私人社交平台的不良言论、负面情绪表达，作为解雇或降薪的理由；部分企业还会要求员工关注企业官方账号、转发企业宣传内容，甚至限制员工在社交平台发布与企业无关的内容。这种对劳动者社交媒体的监视，本质上是对劳动者私人生活安宁权与言论自由的侵犯：劳动者在私人社交平台的表达本应属于个人自由，不应受到用人单位的过度干预；企业将劳动者的私人社交动态与职业评价绑定，迫使劳动者在网络空间也时刻保持“职业形象”，严重压缩了劳动者的私人生活空间。同时，社交媒体数据的采集还可能引发“算法偏见”问题，企业基于劳动者的社交动态构建的画像，可能因算法的不透明性与歧视性，对劳动者产生错误的评价，进而影响其职业发展。

4. 人工智能时代下劳动者隐私权保护的应对

4.1. 完善劳动者隐私权保护的法律法规

应对人工智能时代劳动者隐私权面临的系统性挑战，法律制度的完善是最为基础且关键的路径。当前我国缺乏专门针对劳动者隐私权保护的立法，现有法律条文分散于《个人信息保护法》、《中华人民共和国劳动合同法》(后文简称《劳动合同法》)、《中华人民共和国劳动法》(后文简称《劳动法》)、《民

⁴ 《中华人民共和国个人信息保护法》第 28 条：敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

法典》之中，彼此衔接不畅，且未能充分回应劳动关系中权力不对等的特殊结构。因此，必须从以下方面推进法律体系的专门化重构。第一，在《劳动法》中增设“劳动者个人信息保护”专章。该章节应明确以下核心规则：一是确立用人单位采集劳动者个人信息的“合法、正当、必要与最小必要”原则⁵，禁止超出合理管理需要的过度采集。例如，用人单位不得以考勤为由采集人脸识别信息以外的额外生物特征，不得以绩效管理为由实时监控员工的键盘敲击频率或如厕时长。二是规定用人单位在引入人工智能管理系统前负有强制性的评估义务与告知义务，须向劳动者提供清晰、易懂的隐私政策，明确说明数据采集的类型、目的、保存期限、使用范围以及可能涉及的自动化决策。三是赋予劳动者以具体、可操作的数据权利，包括访问权、更正权、删除权以及拒绝自动化决策的权利。用人单位不得以“技术限制”或“商业秘密”为由拒绝劳动者行使上述权利。第二，建立算法影响评估与备案制度。对于可能对劳动者核心权益，如录用、晋升、解雇、薪酬评定产生重大影响的自动化决策系统，用人单位应当在使用前进行独立的算法影响评估，评估报告应提交劳动监察部门或行业工会备案。评估内容至少应包括：训练数据的来源与代表性、算法是否存在可识别的歧视性偏差、决策逻辑的可解释性程度、劳动者异议机制的设置是否有效等。对于未能通过评估或拒绝接受评估的用人单位，应禁止其使用相关系统。第三，强化法律责任与执法机制。应当显著提高用人单位违规处理劳动者个人信息的处罚标准，形成有效威慑。对于非法采集、泄露或滥用劳动者敏感信息的行为，除民事赔偿外，还应设置行政罚款乃至刑事责任。同时，建议设立专门的劳动领域数据保护执法机构，或赋予现有劳动监察部门以数据执法权限。该机构应配备具备技术调查能力的专业人员，能够穿透算法“黑箱”进行事实查明。此外，应当降低劳动者的举证责任，在劳动者提出初步证据后，由用人单位承担证明其数据采集与算法决策合规的举证责任，以矫正劳资双方在信息与资源上的不对等。通过上述立法完善，可以为劳动者隐私权保护提供坚实的法律底座。

4.2. 规范用人单位知情权的行使

用人单位的知情权是劳动管理中的合法权利。根据我国《劳动合同法》，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，劳动者应当如实说明。然而，人工智能技术的介入使用用人单位的知情权被过度扩张，从“与劳动合同直接相关”的信息延伸至行为轨迹、情绪状态、社交媒体活动乃至生物特征等与工作能力无直接关联的私人领域。因此，必须在法律与制度层面为用人单位知情权的行使划定清晰边界。第一，确立“相关性”与“比例性”双重审查标准。“相关性”标准要求用人单位所采集的信息必须与劳动者的工作能力、岗位职责或劳动安全具有直接关联。例如，对于驾驶员岗位，采集行踪轨迹和驾驶行为数据具有相关性；但对于文案岗位，实时定位员工的行动轨迹则明显超出合理范围。“比例性”标准要求信息的采集范围、频率和侵扰程度与所欲实现的管理目的成比例。如果通过人工抽查、定期汇报等低强度手段即可达到管理目标，则不应采用实时视频监控、生物特征识别等高强度手段。用人单位应当定期对其知情权行使的范围进行内部审查，剔除超出必要限度的数据采集项目。第二，建立“分层同意”机制。对于不同敏感程度的信息，应当设置差异化的同意标准^[7]。对于普通工作信息，可以依据劳动合同或规章制度的概括授权进行采集。对于较为敏感的信息，应当向劳动者作出特别提示，并提供拒绝的选项。对于高度敏感信息，则必须取得劳动者的单独、明示、书面同意，且不得以格式条款一揽子授权。更重要的是，法律应当明确规定：劳动者拒绝提供非必要的敏感信息，用人单位不得因此作出不利对待。只有在“可以说不”的前提下，同意才具有真正的法律效力。第三，强化用人单位的透明度义务与说明义务。用人单位应当制定并向劳动者公开详细的隐私政策，内容至少包括：采集信息的具体类型与目的、数据的存储位置与保存期限、有权访问数据的人员范围、数据共享或委托处理的第三

⁵ 《中华人民共和国个人信息保护法》第6条：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

方名单、劳动者的数据权利及行使方式。对于自动化决策系统⁶，用人单位还应当向劳动者提供通俗易懂的解释说明，使劳动者能够理解算法如何影响其工作评价、薪酬或晋升机会。透明度不是一项道德倡议，而是一项法律义务。违背透明度义务的用人单位，其采集的数据在劳动争议中应当被推定为非法取得，不得作为惩戒或解雇的依据。通过上述规范，可以在保障用人单位正当管理需求的同时，为劳动者隐私权划出不可逾越的底线。

4.3. 加强隐私保护的技术监管

法律规范与企业管理规则的落地，离不开技术层面的支撑与监管。人工智能时代的隐私权保护，不能仅依赖事后的法律责任追究，更需要技术系统的设计、部署与运行阶段嵌入事前与事中的控制机制。加强技术监管，是实现“通过设计保护隐私”理念的核心环节。第一，推广隐私增强技术的应用。隐私增强技术包括联邦学习、差分隐私、多方安全计算、可信执行环境等[8]。这些技术能够在实现数据分析功能的同时，最大限度地避免原始个人数据的集中存储与暴露。例如，在绩效分析场景中，可以采用联邦学习，算法在员工的本地设备上训练，仅上传加密后的模型参数而非原始行为数据，从而在生成群体分析结果的同时保护个体隐私。用人单位在采购或开发人工智能管理系统时，应当优先选择采用隐私增强技术的方案。对于劳动者敏感信息的处理，原则上不得将原始数据集中存储于用人单位可随时访问的服务器中。第二，推动算法的可解释性与可审计性。对于直接影响劳动者核心权益的自动化决策，算法必须具备可解释性。可解释人工智能技术能够将决策逻辑转化为人类可理解的特征贡献度或规则说明。用人单位应当避免使用完全不可解释的“黑箱”算法对劳动者作出不利决策。同时，应当建立算法审计制度，审计内容包括：数据来源的合法性、训练数据是否存在代表性偏差、算法输出是否存在统计上的歧视性差异、决策记录是否完整保存等。审计报告应当向劳动者代表公开，审计中发现的问题应限期整改。第三，建立数据安全事件应急与报告机制。用人单位必须对存储的劳动者个人信息，尤其是敏感信息，采取加密、访问控制、日志审计等安全措施。一旦发生数据泄露或被非法访问，用人单位应当在法定时限内通知受影响的劳动者，并向监管机构报告。此外，监管部门应当建立统一的劳动者隐私投诉与监测平台，利用技术手段对高风险行业和企业进行主动监测。技术监管不是对企业的“不信任”，而是对劳动者权利的必要守护。只有在技术层面建立起有效的约束与监督机制，法律赋予的权利才不会沦为纸面上的空话。

5. 结语

人工智能正在重新书写劳动关系的底层逻辑。效率的追求、管理的便利、技术的可能，正在不断挤压劳动者隐私权的生存空间。智能监控使工作场所趋于透明，敏感信息的过度采集侵蚀着个人边界，社交媒体监视侵扰着私人生活的安宁。而现行法律体系仍在艰难地追赶技术演进的步伐，保护力度明显不足。保护劳动者隐私权不是对技术发展的抗拒，而是对技术异化的必要防范。它维护的是每一个劳动者作为人的尊严与自主性，矫正的是劳资之间日益扩大的权力不对等，构建的是确保技术始终服务于人的制度屏障。这需要在法律、企业、技术与劳动者四个维度上协同发力：通过专门立法确立底线规则，通过企业治理内化伦理要求，通过技术设计实现透明与可问责，通过赋能劳动者激活权利主体。归根结底，这个问题指向一个更根本的追问：在一个算法日益深度介入劳动过程的社会里，我们是否仍然相信——劳动者不仅仅是生产要素，首先是一个拥有尊严、自主与隐私权利的人？对这一追问的回答，将决定人工智能时代劳动关系的伦理底色，也将检验一个社会在技术进步与人文关怀之间寻求平衡的能力与意愿。

⁶ 《中华人民共和国个人信息保护法》第 24 条：个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。

参考文献

- [1] 李学超. 基于人工智能的产品设计理论模型研究[J]. 工业设计, 2020(6): 110-111.
- [2] 向静林. 数字时代的社会巨变与国家治理: 一个整体性分析[J]. 社会, 2025, 45(3): 30-42+1.
- [3] 王利明. 隐私权概念的再界定[J]. 法学家, 2012(1): 108-120+178.
- [4] 孙月月. 人工智能时代隐私权保护的法理学分析[N]. 安徽科技报, 2026-05-13(016).
- [5] 唐湘岚. 人工智能时代劳动权保障的法律困境及其应对[J]. 福建警察学院学报, 2025, 39(4): 99-108.
- [6] 王健. 社交媒体中劳动者隐私权的法律保护——基于欧盟与我国司法实践的比较研究[J]. 华中科技大学学报(社会科学版), 2019, 33(4): 117-125.
- [7] 张文琴. 大数据时代公民隐私权与公共安全之间的法律平衡[J]. 法制博览, 2025(12): 25-27.
- [8] 金俊美. 人工智能时代网络数据信息安全防护策略[C]//重庆市大数据和人工智能产业协会, 重庆建筑编辑部, 重庆市建筑协会. 智慧建筑与智能经济建设学术研讨会论文集(二). 2025: 529-532.