

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

田野^{*}

内容提要 职场智能监控问题愈演愈烈,使劳动者个人信息权益面临更大威胁。数智时代算法权力的失衡使劳动从属性以新的技术面貌呈现并加剧,需加以矫正。在智能监控中,用人单位和劳动者皆有正当而相互冲突的利益存在,如何实现二者的平衡是难点。利益平衡目标的实现应以贯彻目的原则为中心,为智能监控的范围与限度划定边界。基于智能监控处理劳动者个人信息应当具备明确、合理且与劳动直接相关的目的,且以给劳动者造成最小损害为限度。即使是在工作时间和工作场所,也应认可个人信息权益在合乎比例的空间内存在。应当避免持续性、全方位和一般预防性的过度监控,而主要针对工作中的关键时段、场所和有迹象表明违法行为实施有限的监控。鉴于其高度冒犯性,只有在具备重大事由时才能例外地采用智能监控,而不能将其作为监督劳动者工作表现的常规手段。

关键词 职场智能监控 劳动者个人信息保护 劳动从属性 目的原则

目 次

- 一、职场智能监控下的劳动者个人信息危机
- 二、职场智能监控中的权益之争与规范路径
- 三、职场智能监控范围与限度的边界厘定
- 四、结语

^{*} 天津大学法学院教授。本文系 2021 年度最高人民法院司法研究重大课题“平台经济模式下从业者与平台经营者法律关系问题研究”(项目批准号: ZGIFYZDKT202109-01)的阶段性成果。

从世界范围看,用人单位通过智能手环、智能坐垫、监视软件、人体芯片等高科技手段对劳动者实施智能监控,是人工智能时代的一个突出社会问题。^①一方面,人工智能应用于职场有助于提升劳动管理的效率,但另一方面则会对劳动者个人信息构成威胁。职场是个人信息保护的特别场域,其特殊性在于:劳动关系具有从属性特质,劳动者的个人信息权益受到用人单位管理权的制衡。因而,如何平衡用人单位管理权行使中的信息利用与劳动者个人信息保护的关系是焦点和难点。当下对职场智能监控议题的探讨至少有两重特殊意义:一者,探求法律如何因应技术进步,直面人工智能给劳动者个人信息保护带来的挑战;二者,明确在劳动关系中保护个人信息时,法律适用的眼光如何流转于个人信息保护法与劳动法之间。《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)虽可为职场智能监控问题的解决提供基本的规范指引,但具体如何适用,尚需更深入细致的研究。就规制智能监控并消解用人单位和劳动者之间信息利用与保护紧张关系的路径,学者提出了见仁见智的解决方案:有学者从同意及其限制的角度切入寻找利益平衡之道,^②有学者则提出了将个人信息保护纳入劳动基准的设想^③。笔者认为,用人单位基于管理需要对劳动者实施智能监控不可避免,因此对智能监控合法性的判断不是一个全是或全非的问题,关键在于界定信息处理的范围与限度。对此,通过贯彻目的原则对智能监控中信息处理的范围和程度作出限定,或是一条更为直截了当的出路。

一、职场智能监控下的劳动者个人信息危机

职场监控并不是一个新问题,劳动者受监控之苦久矣,只是随着人工智能技术的兴起,用人单位在管理中越来越多地采用智能化手段实施监控,使得劳动者的隐私更加无处遁形。早在1996年,张新宝教授就十分超前地论述了工作场所监视与雇员个人数据保护问题。^④如今,智能监控对劳动者个人信息权益入侵的程度已非昔日可比。

(一) 职场监控方式的智能化发展使劳动者个人信息危机加剧

近年来,国内外职场智能监控热点事件频发,引发了社会极大关注。例如,在国内的“南京环卫工人智能手环”^⑤、“杭州某企业智能坐垫”^⑥等事件中,智能设备能监控劳动者脱岗的时间并自动报告给用人单位。在国外,美国亚马逊公司开发了一套人工智能监工系统对员工的劳动过程实施监控,通过算法对收集到的劳动者个人信息进行分析并形成自动化决策,作为绩效考核乃至解雇的依据,一名女员工甚至因被该智能监控“抓包”

① See Richard A. Bales & Katherine V. W. Stone, *The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace*, Berkeley Journal of Employment and Labor Law, Vol.41:1, p.1-62 (2020).

② 参见吴文芳:《劳动者个人信息处理中同意的适用与限制》,载《中国法学》2022年第1期,第221页。

③ 参见王倩:《作为劳动基准的个人信息保护》,载《中外法学》2022年第1期,第183页。

④ 参见张新宝:《雇员在工作场所的隐私权保护与限制》,载《现代法学》1996年第5期。

⑤ 参见张盖伦:《老套的办法别借智能手环卷土重来》,载《科技日报》2019年4月12日,第7版。

⑥ 参见冯群星:《老板用智能坐垫监视员工,摸鱼早退数据全部掌控?》,载《南方都市报》2021年1月8日,第A12版。

一天上了6次厕所而被解雇。^⑦事后查明,该女员工之所以频繁出入洗手间是因患有的一种肠道应激疾病,这暴露了智能监控的短板。

用人单位出于提升劳动效率、防止财产失窃等考虑而对劳动者进行监视的做法由来已久。在人类社会发展的不同阶段,职场监控方式也有所不同。原始的监控手段主要是人工监控:在雇主能够“看到一切、知道一切、决定一切”的小工厂阶段,最早的职场监控形式是雇主自己亲自上阵监控;第二次工业革命后,这种监控方式面对大规模生产模式越来越捉襟见肘,雇主遂开始选任“工头”作为自己的代理人对工人实施监控。^⑧随着科学技术的进步,职场监控的手段不断翻新:先是摄像头、窃听器等物理监控设备渐渐取代人工监控;之后,无形的电子监控取代了有形的物理监控;^⑨再后来,更先进的数字监控逐渐取代电子监控;而人工智能的出现更增加了职场监控的高科技色彩,使用用人单位的监控能力得到极大提升。据学者考证,从技术迭代的角度看,职场监控已经提升到了“5.0版”,其突出特征就是以数据和算法为支撑的智能化。^⑩其智能突出体现在监控不仅是对劳动者信息进行简单的收集,还能够通过算法自主地对信息作出关联、聚合、挖掘、分析,形成新的数据乃至作出自动化决策。质言之,真正智能的不是手环、坐垫等有形设备本身,而是由用人单位控制的无形算法。

与前几代监控手段相比,智能监控的信息处理能力更加强大,因之对劳动者个人信息权益带来的威胁也更大。第一,智能监控对劳动者个人信息处理的范围更广。打破时空界限的监控无处不在,使得职场与私人生活空间的边界愈发模糊难辨。第二,智能监控对劳动者个人信息处理的程度更深。其不只是单纯获取信息,还通过对信息进行更深度地处理服务于从招聘、考核到解雇等更广泛的管理目标。第三,智能监控的冒犯性更强。传统的监控设备通常安装在劳动者人身之外的工作场所之中,而智能手环、徽章等可穿戴设备则附着于劳动者人体之上,可植入性芯片甚至侵入到人体内部。第四,智能监控的隐蔽性更高。^⑪五花八门的智能监控手段常常以智能化管理为噱头,以不易察觉的方式收集劳动者的个人信息,诸如智能坐垫等监控工具有时还披着关爱劳动者的温情脉脉的外衣。强大的智能监控可轻而易举地形成关于劳动者工作能力和表现的数字画像,使劳动者沦为“数字人”,供老板们选择和操控。

(二) 职场监控法治的迭代演进

在沦为被操控的“数字人”似乎成为数智时代劳动者不可逃脱的宿命之背景下,法

⑦ 参见《亚马逊女员工一天上6次厕所被开除!员工愤而起诉》,载搜狐网, https://www.sohu.com/a/48511-2578_120046968, 2022年4月4日访问。

⑧ 参见姚建华:《作为数据流的劳动者:智能监控的溯源、现状与反思》,载《湖南师范大学社会科学学报》2021年第5期,第93页。

⑨ See Lawrence E. Rothstein, *Privacy or Dignity: Electronic Monitoring in the Workplace*, New York Law School Journal of International and Comparative Law, Vol.19:379, p.379-412 (2000).

⑩ 参见汤晓莹:《算法技术带来的劳动者隐私风险及制度因应》,载《中国人力资源开发》2021年第8期,第66页。

⑪ 参见郑志峰:《人工智能时代的隐私保护》,载《法律科学》2019年第2期,第53页。

律自然不能袖手旁观。之前,法学界的关切点是劳动者的隐私权保护,^⑫随着人工智能与数据时代来临,对职场监控法律议题的关切点正在向劳动者个人信息保护转变^⑬。因为,“工头”时代的职场监控威胁的主要是劳动者在物理空间的有形隐私,而智能监控威胁的则主要是劳动者的无形个人信息。隐私权与个人信息保护的关系错综复杂,两者之交错主要体现在“私密信息”这一点上。^⑭而在数智时代背景下,私密信息恰是法律保护的重中之重,正如有观点认为,“隐私权主要保护的是信息性隐私(information privacy)”^⑮。劳动者个人信息保护蕴含了职场隐私保护,且在语境上与数智时代的背景更加契合。

变迁的不只是学术语境,还有现实世界随监控技术迭代而发展的实在法。保护职场监控中劳动者权利的最初法律进路主要是隐私法。特别是美国法,受其本土法律传统的影响,一直习惯将职场监控放在隐私权框架下解决。欧洲法律对职场监控的规制则较早地从隐私权保护过渡到了个人数据保护的轨道。从1995年的《个人数据保护指令》始,欧盟立法就对雇佣领域的个人数据保护作出了特别规定(但起初并未具体到职场监控这一特定场景),《通用数据保护条例》延续了这一做法。随着高科技监控的问题愈演愈烈,专门针对职场监控的立法开始在全球范围内多点开花,甚至诞生了细化到智能监控领域的特别立法。澳大利亚新南威尔士州早在1998年就通过了《工作场所视频监控法》;欧盟数据保护工作组在2004年发布的《通过视频监控方式处理个人数据的意见》也重点规范了职场监控下的雇员个人数据保护;2019年,美国伊利诺伊州还颁布了《人工智能视频面试法案》,专门针对招聘环节的智能监控加以规范。回溯历史,从隐私保护到个人信息保护,再从个人信息保护法中加入的劳动者个人信息保护特别条款到职场智能监控专门立法,职场监控法律治理日益精细化。

二、职场智能监控中的权益之争与规范路径

个人信息保护中的主要矛盾是信息利用与个人权益维护的冲突,^⑯这一点在劳动场景下体现得尤为淋漓尽致。一方面,基于管理需要,用人单位以智能监控等方式处理劳动者个人信息似乎有着天然的正当性;另一方面,劳动者的人格尊严也不应因为其置身职场而彻底丧失。当二者激烈交锋时,信息利用与保护的紧张关系遂不可避免地发生。

^⑫ See Arthur P. Menard & Anne K. Morrill, *The Employer and the Law of Privacy in the Workplace —The U.S. Model to Date*, North Carolina Journal of International Law, Vol.9:93, p.93-116 (1983). 我国学界对劳动者隐私权保护也有一定程度的研究。参见喻术红、汤晓莹:《劳动者隐私保护问题研究现状及其评述》,载《时代法学》2020年第5期。

^⑬ 参见谢增毅:《劳动者个人信息保护的法律效力、基本原则及立法路径》,载《比较法研究》2021年第3期,第26页。笔者认为,从整个民法人格权发展的轨迹来看,个人信息保护之所以逐渐获得独立的地位,乃是时代发展使然,而从隐私到劳动者个人信息保护的变迁正是该发展趋势的一个缩影。

^⑭ 参见程啸:《个人信息保护法理解与适用》,中国法制出版社2021年版,第38-40页。

^⑮ 吴伟光:《从隐私利益的产生和本质来理解中国隐私权制度的特殊性》,载《当代法学》2017年第4期,第55页。

^⑯ 个人信息利用与保护的矛盾关系在《个人信息保护法》第1条规定的立法目的中有明确体现。参见张新宝主编:《〈中华人民共和国个人信息保护法〉释义》,人民出版社2021年版,第22页。

笔者认为,究其根源,乃在于劳动关系的从属性特质。

(一) 用人单位实施智能监控的权源和理据

人工智能在劳动管理中的应用日益普及,而用人单位热衷于智能监控的背后有着复杂的因素。在智能监控中,用人单位确实有着一些攸关的利益需要保护。

1. 用人单位的管理权

管理权是用人单位实施智能监控的首要依据。用人单位有权指挥管理劳动者,在这一点上不存在太大争议。^{①7}管理的智能化有利于提升管理的效率,因而是社会发展的大势所趋。一个实例是,美国UPS公司在每辆运输车上安装了200多个传感器用于追踪路线、速度、停车、包裹提取、扣安全带用时等详细信息,统计表明,公司借此在1年时间里节省了170万英里行驶里程、1500万分钟时间、103000加仑汽油。^{①8}我国《个人信息保护法》第13条第1款第2项将“实施人力资源管理所必需”列为个人信息处理的合理情形之一,正是对用人单位基于管理权处理劳动者个人信息的明确肯认。在司法实践中,面对劳动者提出的监控侵权之主张,用人单位常采用的管理权之抗辩理由也多为法院所认可。例如,在一个雇员与公司的隐私权纠纷案件中,被告公司通过对原告工作手机的定位进行监视。法院分析认为,原告作为营销人员,其工作岗位具有流动性大的特点,被告公司作为用人单位对其手机开通翼定位群服务,是对员工进行管理监督的手段之一,没有证据证明原告因此遭受了伤害,因此被告公司的行为不构成对其隐私权的侵犯。^{①9}

2. 用人单位财产权

用人单位实施智能监控,也可能是为了维护本单位的财产安全。首先,劳动工具和生产资料为用人单位所有,用人单位当然有权监督这些工具和资料如何被使用,并确保这些财产的安全。其次,劳动生产出来的产品归用人单位所有,智能监控亦可防止这些产品被偷窃。最后,用人单位享有的商业秘密以及其他知识产权,也常常需要借助智能监控手段予以保护。在司法实践中,财产权是人民法院作出有利于用人单位裁判常常援引的理由。例如,有的法院就在判决中明确提出,被告公司作为经营办公场所及设施的所有权人,对其场所和设施享有管理权和支配权。^{②0}

3. 用人单位的义务与责任风险

根据《个人信息保护法》第13条第1款第3项,如果是“为履行法定职责或者法定义务所必需”,则可以处理个人信息。用人单位实施智能监控可能是为了履行法定义务,或者是规避承担法律责任的风险。例如,劳动法领域最典型的用人单位法定义务就是职场安全健康维护义务。如果智能监控收集劳动者个人信息是以维护职场安全健康为目的,则监控行为不仅不违法,还是用人单位善尽义务应为之行为。又如,根据《民法

^{①7} 参见田思路:《智能化劳动管理与劳动者隐私权的法律保护》,载《湖湘论坛》2019年第2期,第16页。

^{①8} See Wes Turner, *Chipping Away at Workplace Privacy: The Implantation of RFID Microchips and Erosion of Employee Privacy*, Washington University Journal of Law & Policy, Vol.61:275, p.276 (2020).

^{①9} 参见广东省中山市第一人民法院(2017)粤2071民初5281号民事判决书。

^{②0} 参见上海市静安区人民法院(2017)沪0106民初17104号民事判决书。

典》第 1010 条第 2 款,用人单位负有防治职场性骚扰的义务,而智能监控也是防治职场性骚扰的有效手段。此外,很多用人单位实施针对劳动者社交媒体的监控之目的在于防止因劳动者在社交媒体上的违法言论“引火上身”。如在 *Otomewo v. Carphone Warehouse Ltd.* 案中,一公司就因两名员工在同事的 Facebook 页面下发表了关于其性取向的不当言论而被追究法律责任,理由是这些违法行为发生在工作时间。^{②①}

(二) 管理权挤压下的劳动者个人信息权益

为了从用人单位换取生存所需之报酬,劳动者让渡出了一部分权益。但此种退让应当是有限度的,不能被简单化地理解为人格减等。用人单位对劳动者个人信息的智能化监控贯穿收集、存储、使用、提供、公开等个人信息生命周期的各个环节,使劳动者面临多种被侵害的风险——包括个人信息权益的直接损害以及由此衍生的周边权益的损害等。

从内部构造来看,个人信息权益包含个人信息的“本权权益”和“保护本权权益的权利”。^{②②}对劳动者个人信息“本权权益”的损害大体包括三个方面:(1)劳动者的人格尊严。其一,隐私暴露。智能监控会使那些不为人知的劳动者私密信息暴露于外,此种情况构成侵犯隐私权和侵犯个人信息权益的竞合。其二,算法歧视。用人单位常常基于智能监控收集到的信息对劳动者作出评价,甚至于由人工智能自动形成惩戒或解雇的指令。由于人工智能和算法的局限性,自动生成的决定可能是草率和歧视性的。其三,一般人格权损害。高强度智能监控的职场环境可能使劳动者陷入持续的紧张、焦虑之中,使劳动丧失体面和尊严,这可认为是对劳动者一般人格权的侵害。(2)劳动者的通信自由和通信秘密。用人单位对劳动者的电话、邮箱、微信等通信方式和社交媒体实施智能监控,可能构成对通信自由权和通信秘密权的侵害。(3)劳动者的人身财产安全。用人单位不当泄露智能监控获取的劳动者个人信息,后续可能导致劳动者因身份窃用、诈骗等遭受人身或财产损害。就“保护本权权益的权利”而言,由于实践中大量的职场智能监控都是秘密实施的,劳动者的知情权、决定权等也可能因非法的智能监控而受到侵害。

除了侵害劳动者个人信息权益外,非正当的智能监控还可能对劳动者在劳动法上的诸多权利构成侵害。例如,算法歧视对劳动者的平等就业权构成侵害;不公正的自动化决策导致劳动者降薪,使其获得公平劳动报酬权受到侵害;不间断且无死角的监控使劳动者陷入持续的紧张焦虑之中,使劳动者在精神卫生方面的职业安全健康权受到侵害;失准的自动化解雇决策让劳动者失去饭碗,使其职业安定权受到侵害;等等。可见,针对智能监控,劳动者有跨越不同部门法的广泛权益需要被维护,而现实中,这些权益的存在空间却因受到用人单位过度监控的挤压而不断萎缩。

(三) 劳动从属性下的算法权力失衡与矫正

劳动关系是一种不平等的法律关系,^{②③}由此决定了其法律调整方法的独特性——以

^{②①} See *Otomewo v. Carphone Warehouse Ltd.*, [2011] ET 2330554.

^{②②} 参见张新宝:《论个人信息权益的构造》,载《中外法学》2021 年第 5 期,第 1144 页。

^{②③} 劳动关系与其他不平等关系(如消费者和经营者之间的关系)有微妙的不同:其不平等性是与生俱来的,是保证用人单位指挥管理业务正常运转所必需的。

倾斜保护为要旨^{②4}。劳动关系的不平等特征被提炼为“劳动从属性”。一般而言,劳动从属性可细分为三个层面:一是组织从属性,劳动者被纳入用人单位的组织体系而成为其中一员,就像庞大机器上的一个螺丝;二是人格从属性,在劳动中,用人单位得对劳动者发号施令及实施监督管理;三是经济从属性,劳动者仰赖用人单位发放的报酬作为生存之经济来源。^{②5}这种从属性决定了在劳动关系框架下用人单位和劳动者权利义务配置的基本格局,也是判断职场智能监控合法性的基本出发点。由于从属性的劳动关系与以平等自治为精神内核的民事关系显有不同,两者在个人信息保护方面亦存在诸多差别。如果说个人信息保护法所调整的处理者(多为实力强大的企业)与个人之间的关系本身就是一种源于信息不对称的不平等关系,那么劳动关系的从属性无疑使不平等的程度“更上一层楼”,因此劳动者在众多信息主体中作为“弱者中的弱者”更需要得到特殊关怀。

进入数智时代,强资本弱劳动的格局并未发生逆转性改变,相反,由于用人单位的“武器库”中增加了智能监控这一新的高科技“装备”,劳动从属性非但没有降低还有所增强。凭借智能监控,用人单位得以更加广泛深入地收集处理劳动者个人信息,劳动从属性更得以以“算法从属性”的新态样呈现。若从更深层面反思,这其实是算法权力失衡在劳动场域下加强的表征。当下,算法正在形塑一种新的权力秩序^{②6}:算法精英凭借科技优势掌控算法权力,而受制于知识能力劣势的个人则有沦为“算法囚徒”的风险^{②7}。在劳动场域下,基于算法的管理反映了数智时代劳动管理的全新面貌(智能监控正是其具体表现形式之一),在此面貌之下,用人单位就是算法精英,而劳动者则成为受困于职场的“算法囚徒”。因此,笔者认为,在劳动管理日趋智能化的背景下,有必要于传统的组织从属性、人格从属性和经济从属性之外,承认“算法从属性”。

劳动从属性之“人工智能加强版”必然给劳动者个人信息保护带来巨大影响,这也决定了对职场智能监控应当采取的根本法律立场。辩证地看,这种影响起码体现在以下相互制约的两个方面。一方面,劳动从属性为用人单位实施智能监控提供了必要的正当性基础,在用人单位管理权面前,劳动者的个人信息权益不得不作出一定的退让。但法律调整的目标不在于彻底消灭不对等的法律关系,也不在于使劳动者获得与用人单位相同的算法权力,而在于矫治那些不合理的不对等以及由此导致的过度失衡。对职场智能监控不应一棒子打死,而应容许其在合理限度内存在。另一方面,劳动从属性本就将劳动者个人信息权益置于较大的风险之中,而智能化又使之雪上加霜。但从属性不应产生使劳动者人格权归零的效果,即使是在工作时间和工作场所,劳动者亦享有包括个人信息权益在内的人格权益不受侵犯的权利。^{②8}因此,应对劳动从属性作出必要限制,对智能

②4 参见丁晓东:《法律如何调整不平等关系?论倾斜保护型法的法理基础与制度框架》,载《中外法学》2022年第2期,第445—464页。

②5 参见肖竹:《劳动关系从属性认定标准的理论解释与体系构成》,载《法学》2021年第2期,第160页。

②6 参见张凌寒:《算法权力的兴起、异化及法律规制》,载《法商研究》2019年第4期,第63页。

②7 参见彭兰:《算法社会的“囚徒”风险》,载《全球传媒学刊》2021年第1期,第3页。

②8 参见田野:《雇员基因信息保护的私法进路》,载《法商研究》2021年第1期,第54页。

监控下的算法权力失衡进行矫正。以上两面性决定了智能监控中劳动者个人信息保护问题的特殊性：用人单位实施的智能监控有其合理性的一面，但并不总是如此。由此，问题的关键就归结为：职场智能监控的合理边界如何划定？哪些监控可以被认可，哪些又应被禁止？

从更具体的层面来看，从属性对劳动者个人信息保护的影响还体现在对规范路径侧重点的选择。最明显的影响就是同意规则的适用困境。在个人信息保护法上，同意是个人信息处理最一般化的合法性基础，然而其在劳动领域阻力重重。受劳动从属性影响，在缺乏议价能力情况下之同意的真正自愿难以确保。即使智能监控形式上经过了劳动者的同意，但由于其可能是劳动者迫于生存压力而作出的，其真意表达的可信度大打折扣。^{②⑨}正因如此，有学者认为，在劳动领域内，同意不能独自作为信息处理的正当性基础，而应转向对处理行为本身正当性的判断。^{③⑩}同意不是没有意义的，但只有同意可能是不够的。^{③⑪}在同意规则失灵之后，对职场智能监控问题的解决应寄希望于对监控行为本身正当性的判断，而对监控的目的及其范围作出限定则是确保监控行为合法正当最直接有效的规范手段。

三、职场智能监控范围与限度的边界厘定

职场智能监控法律治理的关键在于划界，然适度与过度之间并非泾渭分明，要破解划界难题仍需从个人信息保护法寻找答案。个人信息保护法之各项基本原则对职场智能监控皆得适用自不待言，然若从对症下药治理过度监控的问题导向出发，目的原则最为契合。

（一）目的原则的边界厘定与利益平衡功能

用人单位对劳动者实施智能监控必须具有明确、合理的目的，这是最基本的要求。《个人信息保护法》第6条规定：“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。”该条确立了目的原则，其内部又可细分为目的限制原则和最小化原则两项子原则。域外的一些个人信息保护立法将二者分别列为两项原则，如欧盟《通用数据保护条例》第5条第1款（b）项规定了目的限制原则，（c）项紧接着规定了最小化原则。鉴于最小化与目的的密切联系，我国《个人信息保护法》将目的限制与最小化合并规定于同一条文中，由二者协同决定信息处理的范围广度和深度边界。对职场智能监控正当边界的厘定，亦应从这两个基本方面切入。

《个人信息保护法》第5-9条集中规定了五项基本原则：合法、正当、必要和诚信原则；目的原则；公开、透明原则；质量原则；责任原则。这五项原则并非彼此割裂而是相

^{②⑨} 参见前注③，王倩文，第185页。

^{③⑩} 参见前注⑬，谢增毅文，第35页。

^{③⑪} See Antonio Aloisi & Elena Gramano, *Artificial Intelligence Is Watching You at Work: Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context*, Comparative Labor Law & Policy Journal, Vol.41(1):95, p.105 (2019).

互协同的,彼此间有一定的位阶关系,共同构成完整的原则体系。其中,合法、正当、必要和诚信原则是总体性原则,抽象程度最高,主要发挥价值指引功能;后四项是具体原则,各有侧重,是总体原则的展开。^③在诸具体原则中,目的原则的意义尤为重大,占据核心地位。从规定顺序来看,目的原则紧跟总体性原则之后,列于各项具体原则之首,承上启下。承上体现在目的原则是总体原则的具体化展开,所谓“合法、正当、必要”,首先是就目的而言的;启下体现在目的原则引出其他具体原则,具有前提性、基础性意义。职场智能监控如果连明确的目的都不具备或者目的不合理,则在合法性入口处就被“拒之门外”,根本没有必要进入到“公开、透明原则”“质量原则”和“责任原则”层面的讨论。此外,目的还决定公开透明的对象范围,突出体现在告知义务的事项设置上——根据《个人信息保护法》第17条第1款第2项,“个人信息处理目的”是处理者应向信息主体告知的核心事项。进而,目的还决定同意有效的范围,根据《个人信息保护法》第14条,处理行为超出目的范围则需重新获得同意。由是观之,“目的”实为个人信息处理的“轴心”。

从作用机理来看,目的原则的直接功能就在于从广度和深度两个方面框定个人信息处理的边界,并进而实现处理者和信息主体之间的利益平衡。具体到智能监控场景,用人单位是否可以对劳动者实施智能监控,在根本上是由监控目的有无及其合理性决定的,而目的范围的宽窄则直接影响双方当事人具体权利义务配置的天平。应当看到,个人信息保护法既是认定不正当的处理行为违法而保护个人信息的法,同时也是认定处理行为合法而为正当的信息利用行为保驾护航的法。包括智能监控在内的信息处理行为只要不逾越底线,即可获得法律的认可,阻却法律责任的承担。因而,目的原则所框定的边界,既是用人单位管理权的边界,也是劳动者个人信息权益的边界,同时还是法律责任的边界。在合理目的范围内实施监控,用人单位就能够实现其管理需求并(在不违反其他原则的前提下)免于承担法律责任,劳动者的个人信息权益也能得到维护,双方各取所需从而实现利益平衡;超出目的实施智能监控时,用人单位则须根据超出目的范围的程度承担相应的法律责任。从这个意义上讲,合理目的之所在也就是最佳利益平衡点之所在。

(二) 智能监控中的目的限制原则

关于目的要求,欧盟《通用数据保护条例》第5条用了三个限定词描述,即“特定”(specified)、“明确”(explicit)和“合法”(legitimate);我国《个人信息保护法》第6条则采用了“明确”“合理”以及“直接相关”的表述。在职场智能监控场景下,对合乎要求的目的之判断,需从以下几方面细致分析。

第一,监控目的明确。用人单位不能通过智能监控漫无目的地预先收集存储劳动者个人信息,留待以后需要时使用。对监控目的的描述应当具有清晰的指向性,不能采取隐秘、模糊及高度抽象的方式。实践中,用人单位常采用“为提高员工劳动效率”“为维护本单位财产安全”等十分模糊的表述,还有的用人单位规章甚至不明确提及可能实施智能监控。这种模糊不清的目的实际上就是没有目的。

^③ 参见张新宝:《个人信息处理的基本原则》,载《中国法律评论》2021年第5期,第18页。

值得特别探讨是,智能监控的目的是否必须特定?如前述,欧盟《通用数据保护条例》要求目的特定,而我国无论是《民法典》还是《个人信息保护法》均未对目的特定作出一般性的规定。这是否意味着个人信息处理的目的可以不特定呢?有观点认为,须将目的特定与明确、合理并列为要求。^{③③}笔者认为,可从以下两个角度辩证看待这一问题:一方面,“明确”在一定意义上涵盖了“特定”,“特定”是“明确”的题中应有之义。例如,程啸教授就认为,“明确”包含两层含义,一是表达清晰、不模糊,二是范围有限定。^{③④}另一方面,个人信息的类型不同,敏感程度存在差异,对目的特定的程度要求也可能存在差异,不宜僵化地一刀切。《个人信息保护法》第28条第2款规定:“只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,个人信息处理者方可处理敏感个人信息。”该条款针对敏感个人信息处理明确规定了“特定”要求,彰显了更高层级的保护。^{③⑤}结合该条款和第6条作体系解释,可大概揣测立法者的意图,即根据信息类型的差异而课以不同的特定性要求,以实现利用与保护之平衡。职场智能监控若是针对一般个人信息,则所限定目的之描述可以具有一定的概括性;但若是针对敏感个人信息,则目的必须是特定的。

第二,监控目的合理。目的合理建立在合法基础上,但合法的目的不一定都合理。^{③⑥}在智能监控场景下,对目的合理性的判断主要应以总体性原则中的正当原则和必要原则为价值指引,从监控行为所欲实现的利益是否正当且必要加以判断。若智能监控是为了劳动者的利益,如预防职业病等,则目的是合理的。更普遍的情况是,用人单位实施监控是为了自己的利益,如提升工作效率、维护财产安全等,这些目的总体上也可以说是合理的。但若智能监控只是为了刺探劳动者隐私,则目的不具有合理性。

第三,监控目的与劳动直接相关。《个人信息保护法》第6条明确采用了“直接相关”的表述,这是对处理行为与目的关联性的严格要求。“直接”意味着强关联,如果处理行为与目的之间无关联或只是间接相关,则不满足要求。依此,处理者亦不得实施超出初始目的的后续处理,除非重新取得同意或具备其他合法事由。^{③⑦}具体到智能监控场景,即通过智能监控处理劳动者个人信息必须与工作直接相关。

在实践中,对智能监控目的的相关性应结合监控获取的个人信息类型、劳动者工作的内容等因素进行判断。例如,网络配送平台企业监控骑手的位置行踪信息,是为了便于算法智能化计算送货路线、时间,找到效率最大化的匹配方案,即可认为是与工作目的直接相关的处理;而监控骑手的微信等社交媒体上的个人信息,则与管理骑手的工作没有紧密的相关性。对智能监控相关性的判断有时会遭遇困难。例如,用人单位监控社交

^{③③} 参见刘权:《论个人信息处理的合法、正当、必要原则》,载《法学家》2021年第5期,第8页。

^{③④} 参见程啸:《论我国个人信息保护法的基本原则》,载《国家检察官学院学报》2021年第5期,第11页。

^{③⑤} 参见王利明:《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》,载《当代法学》2022年第1期,第11页。

^{③⑥} 参见前注^{③④},程啸文,第12页。

^{③⑦} 参见前注^{③⑥},张新宝文,第22页。

媒体可能是为了避免员工不当行为诱发用工者侵权责任——这样的担忧并非完全是杞人忧天,相关案例确有发生^{③⑧}。但笔者认为,对相关性不能作普遍联系式的宽泛解释,社交媒体监控与雇佣活动的相关性虽并非全无,但总体而言较低,不满足“直接相关”标准,除非其监控的是专门用于与客户沟通的办公社交媒体账号。

(三) 智能监控中的最小化原则

用人单位实施智能监控处理劳动者个人信息,应以满足管理目的需要的最低限度为标准,以给劳动者造成最小损害为尺度。最小化是前述总体性原则中必要原则的直接体现,也是目的原则的重要组成部分。按照最小化的精神,对个人信息能不处理尽量不处理,能少处理尽量少处理,如果处理不可避免,那么以给信息主体造成最小损害的方式处理。《个人信息保护法》第6条两次提及“最小”:第1款规定,处理个人信息应当“采取对个人权益影响最小的方式”,其中的“最小”针对的是对个人权益的影响,约束的是信息处理的方式,适用对象是各种处理行为,涵摄性更强;第2款规定,“收集个人信息,应当限于实现处理目的的最小范围”,“最小”则是仅针对信息收集行为,适用对象更加聚焦。^{③⑨}

对职场智能监控的法律治理而言,最小化具有至关重要的意义,因为实践中职场智能监控问题的症结恰恰在于过度监控。最小化的判断是一个主要难点。怎样的智能监控就是符合最小化标准的?对此没有简单易行的标准公式。笔者认为,用人单位对待智能监控应持如履薄冰的克制立场,最小化与否应当向目的看齐。概言之,被监控收集的个人信息对于用人单位而言应当是实现管理目的必不可少的,只要用人单位的监控目的达到了,就不应再收集更多的个人信息了。具体而言,智能监控是否遵循了最小化要求,可大体从以下六个方面加以判断:(1)是否存在其他对劳动者个人信息权益损害更小的替代方式。例如,如果是为了考勤的目的,则安装具有人脸识别功能的监控摄像头并不必要,因为签到、打卡等传统方式也足以实现该目的。即便同为智能监控,各方式之间对个人尊严的冒犯性程度也是存在高低差异的。安装在车辆、电脑等办公设备上的监控设备比智能手环等安装在劳动者身上的监控设备冒犯性更低,而智能手环等外部穿戴的监控设备比植入皮下的微芯片监控冒犯性更低,因为前者可以自由去除,后者则否。用人单位应优先选择冒犯性最低的监控方式。(2)监控时间限制。智能监控原则上只能在工作时间实施,24小时的全天候监控显然不符合最小化要求。在 *Cunningham v. New York Department of Labor* 案中,原告的私人汽车被雇主安装了GPS追踪设备,受到每周7天、每天24小时的不间断监控,纽约州法院认为监控超出了必要限度。^{④⑩}即使是在工作时间,也应尽量避免持续监控,而应只针对工作流程中的某些敏感环节(如涉及现金交接的时段等)进行监控。(3)监控空间限制。智能监控不能无处不在,原则上只能在工作场所实施,而不能延伸至劳动者的家庭等私人空间。即使是在工作场所,也应尽量避

^{③⑧} See *Otomewo v. Carphone Warehouse Ltd.*, *supra* note 21.

^{③⑨} 参见前注^{③④},程啸文,第13页。

^{④⑩} See *Cunningham v. New York Department of Labor*, 997 N.E.2d 468, 470 (N.Y. 2013).

免全面监控,而只能针对某些存在风险的敏感位置(如收银柜台等)进行监控。相比于工作场所的公共开放空间(如大厅、走廊等),在相对密闭的空间(如个人办公室及文件柜等),劳动者有更强的隐私期待,因而不宜监控。在 *O'Connor v. Ortega* 案中,一名雇员涉嫌性骚扰,雇主监视搜查了其办公桌和文件柜,美国最高法院认为这侵犯了该雇员的隐私。^① 此外,对于洗手间、更衣室等敏感私密空间原则上禁止安装监控。对此,欧盟数据保护工作组 2004 年发布的《通过视频监控方式处理个人数据的意见》中即有明确规定。(4) 信息类型限制。用人单位对劳动者的一般信息有更大的监控权,但对于生物识别信息等敏感个人信息则原则上不得监控,除非有特别的正当理由。例如,美国《基因信息反歧视法》对雇主收集雇员的基因信息原则上加以禁止,为数不多的例外主要限于为了维护职场安全健康的目的。(5) 信息数量限制。用人单位应尽可能少地收集劳动者个人信息,以满足特定人力资源管理目的需要为限。(6) 保存期限限制。根据《个人信息保护法》第 19 条,用人单位对监控收集的劳动者个人信息的保存期限应当为实现处理目的所必要的最短时间。

(四) 智能监控合法性判断中的动态利益衡量

如上所述,就职场智能监控中如何寻找用人单位和劳动者利益的最佳平衡点,目的原则提供了利益衡量所需的核心标准——目的明确、合理、直接相关与处理最小化,而在实际的法律适用中对这些标准的具体运用是一个动态的平衡过程。基本的着眼点在于:对用人单位因监控而得到的利益和劳动者因监控而面临的风险进行比较,二者应当是成适当比例的。这一平衡思想被形象地提炼为“比例原则”。我国《个人信息保护法》虽未将比例原则明确规定为法定原则,但是实质认可了比例原则的精神价值,并将其融入于目的原则之中。在个人信息保护中,比例原则的基本含义是个人信息处理的手段、程度与目的成比例,处理者的利益与个人承受的损害成比例。这与目的限制和最小化不谋而合。可以说,比例原则的动态适用也就是目的原则的贯彻过程。

按照比例原则的精神,首先承认信息处理者和信息主体都有正当的利益,进而通过对双方的利益风险进行权衡比较,决定哪一个是应受更优先保护的利益。比例原则的精髓在于利益衡量,特别适用于那些需对若干冲突的利益作出取舍之情形。在职场智能监控场景下,用人单位的管理权与劳动者的个人信息权益发生激烈碰撞,利益平衡的需求比一般的个人信息保护场景更为迫切。例如,欧盟数据保护工作组 2017 年发布的《职场数据处理意见》(Opinion 2/2017 on Data Processing at Work)就指出,应通过描述新技术带来的挑战,使用比例原则对新出现的情况进行评估,对雇主合法利益与雇员隐私期待的平衡作出新的评估。有学者认为:“比例原则成为各国职场个人信息保护法的核心原则,甚至可以称之为‘帝王条款’。”^②

比例原则也被法院运用于职场监视案件的审判。在 *Nikon France v. Frederic Onof*

^① See *O'Connor v. Ortega*, 480 U.S. 709, 711–12 (1987).

^② 前注^⑬,谢增毅文,第 32 页。

案中,雇主监视并复制了雇员的电子邮件,结果发现其利用办公电脑从事了雇主明确禁止的私人活动。法国最高法院认为,雇主对雇员电子邮件不受限制地获取是不合理的,雇员偶尔使用办公电脑收发私人邮件是不可避免和可接受的,即使是在工作时间、工作场所以及雇主明确禁止将办公电脑挪作私用的情况下。^{④③} 该案是较早地将比例原则适用于职场监控领域的经典案例,这一判决意义非凡,宣示了即使是在工作时间和工作场所亦应为劳动者保留适度的隐私空间。在新近的 *Barbulescu v. Romania* 案中,比例原则的精神得到了传承。该案原告 Barbulescu 是销售人员,应公司要求注册了一个 Yahoo Messenger 账号,以满足与客户联系的需要。公司的内部规章规定,禁止员工将公司办公资源用于私人目的,但并未明示可能实施监视活动。公司未经告知同意对原告使用 Yahoo Messenger 的情况进行了监视,发现原告在工作时间利用该软件进行了大量与工作无关的聊天。公司在监视过程中收集下载的文本信息还包含了一些诸如性话题等高度私密的敏感个人信息。原告的诉讼之路非常艰辛,穷尽了罗马尼亚的一切国内诉讼程序仍未获得成功。罗马尼亚各级法院给出的理由是,原告就职的公司对其享有管理权,既然原告否认其占用公司资源从事私人事务,那么公司监视查看其在 Yahoo Messenger 的交流内容就成为查清事实的唯一途径,因此这一行为并不违法。Barbulescu 继续将官司打到了欧洲人权法院并最终获得了成功。欧洲人权法院根据《欧洲人权公约》第8条作出了最终判决,认定罗马尼亚没有为原告的私人、家庭生活、通信应获尊重权提供足够有效的保护,没有处理好相关者利益的平衡。法院认可雇员在工作场所也享有私人生活受尊重的权利,无论雇员是否有隐私期待。^{④④} 这一判决具有风向标意义,警示欧洲范围内的雇主在实施职场监控时必须制定明确细致的监控政策,并向雇员履行充分告知义务。^{④⑤}

相比国外法院对比例原则的开明立场,我国法院则显得较为保守,在面对类似的职场监控案件时,人民法院较少在用人单位和劳动者之间进行细致的利益风险衡量,而大多倾向于以用人单位享有管理权为由径直认定监控行为合法。例如在“修玉婵与海阳市融昌塑编包装有限公司隐私权纠纷案”中,融昌公司在其交付给修玉婵使用的办公电脑上安装了“超级眼”电脑监控软件,并用该软件自动下载修玉婵的微信、QQ等社交媒体上的聊天信息。两审法院均认为,修玉婵在工作期间应该忠于职守,公司提供的办公电脑应仅用于公司安排的工作任务,不应用于除工作业务之外的其他用途;其办公电脑内的使用空间对于公司来说是公开的,不构成秘密,融昌公司在其所有的办公电脑上安装“超级眼”电脑监控属于企业的自我管理行为。^{④⑥} 这样的判决推理过于简陋,其背后

^{④③} See Evisa Kambellari, *Employee E-mail Monitoring and Workplace Privacy in the European Perspective*, Iustinianus Primus Law Review, Vol.5(1):1, p.10(2014).

^{④④} See Joe Atkinson, *Workplace Monitoring and the Right to Private Life at Work*, The Modern Law Review, Vol.81(4):688, p.690(2018).

^{④⑤} See Corneliu Birsan & Laura-Cristiana Spataru-Negura, *Workplace Surveillance: Big Brother Is Watching You*, Lex ET Scientia International Journal, Vol.25(1):50, p.63(2018).

^{④⑥} 参见山东省烟台市中级人民法院(2019)鲁06民终7145号民事判决书。

的简单逻辑就是用用人单位的管理权排除劳动者的一切隐私期待,工作场所之内、工作设备之上无隐私。在很多监控类案件中,用人单位通过秘密监控确实发现了劳动者有严重违规行为,且该行为可能确实满足了劳动法上解雇的要件,但这能治愈秘密监控在程序上的违法性吗?这颇有点“毒树之果”的意思。“Barbulescu 案”和“修玉婵案”皆是这样的状况。不同的是,欧洲人权法院在前案中采取了对劳动者有利的立场;我国法院则对后案采取了相反的立场,以在后发现的修玉婵违反劳动规章制度事实倒推在先的秘密的社交媒体智能监控行为合法,但这样的判决漠视了比例原则,过度偏向了用人单位的管理权而牺牲了劳动者的人格尊严利益。未来,我国法院在面对职场智能监控案件时,应对比例原则多加重视,肯定劳动者在劳动关系下亦享有相当程度的个人信息权益。^{④⑦}

具体而言,对职场智能监控是否符合比例原则的认定需在个案中综合考量各种因素,并按照三阶段检测法分步骤进行。欧洲人权法院在“Barbulescu 案”中归纳了五个方面的判断因素:(1)事先是否告知;(2)监控行为的侵犯性(intrusiveness)程度;(3)雇主是否有正当的原因和需保护的利益;(4)劳动者因监控可能受到的损害后果;(5)程序性保障措施是否到位。这些列举具有借鉴意义,但显然未穷尽一切要素,确定合理比例判断要素及其灵活运用只能放在个案中进行。就比例原则适用的流程而言,通常有三个检测步骤,即适当性(suitability)、必要性(necessity)和利益风险比较(狭义比例)。以在捷克发生的一起职场监控案件为例,雇主对长途客车司机及售票员实施了摄像头监控,理由是为维护乘客生命安全和自己的财产(汽车和票款)安全。法院在判决中首先对适当性问题进行了检测,认为摄像头监控对于预设目标确实能起到一定的预防作用,因此第一阶段的检测通过。在第二阶段的检测中,法院认为,雇主实施的监控是贯穿工作时间始终的,冒犯性较强,而如果只针对特定敏感时间段(如收银)和特定区域(如司机驾驶舱)实施监控,则是冒犯性更低而同样奏效的合理方式,雇主没能证明采用其他冒犯性更低的方式不奏效,因此必要性检测不通过。因为第二阶段的必要性检测没有通过,所以法院放弃了第三阶段的检测。^{④⑧}如果要将该阶段的狭义比例检测补全,那就是:雇主的持续全方位监控完全碾压了雇员权益,没有满足最低限度保护的要求。

(五) 职场智能监控正当目的之类型化判断

以上是关于职场智能监控中目的原则适用的一般化分析,若要最大限度消除目的原则适用的模糊性,尚有必要深入到更加具体的监控场景加以分析。现实中智能监控的态样五花八门,所欲实现的劳动管理目的存在差异,其合法性亦不可一概而论。在此情况下,根据具体场景将智能监控予以类型化,有助于提升法律分析和适用的精确化程度。

类型一:为发现犯罪而实施的智能监控。在一般意义上,此种监控的目的是正当的,不过也不能采无限宽泛的解释。在没有任何迹象表明犯罪已发生或可能发生的情况下,

^{④⑦} 我国法院的个别判决也隐约带有一些比例原则的影子。参见北京市第二中级人民法院(2018)京02民终970号民事判决书。

^{④⑧} See Václav Šmejkal, *High Tech Monitoring versus Privacy in the Workplace in the Law and Case Law of the Czech Republic*, Białostockie Studia Prawnicze, Vol.24:53, p.66-70 (2019).

纯粹是为一般性预防犯罪目的而在职场实施智能监控不应当被认定为合法。根据德国《联邦数据保护法》第26条第1款,只有针对那些有事实和证据表明的犯罪,才能处理劳动者的个人数据。实践中,德国数据保护局也认为,即便是为了防止和调查犯罪行为,公司也应该首先采取比监控更为温和的手段,除非是对特定人员有合理的怀疑。^{④⑨}

类型二:为维护职场安全健康的智能监控。如果监控是为了防止某种职业病或者伤害事故的发生,则受益者是劳动者本人,其监控目的总体而言具有正当性。不过“职场安全健康”是十分笼统的表述,用人单位必须证明潜在的安全健康风险具体指什么,以及风险程度有多高。通常,风险应与工作岗位的性质密切相关,且只有那些确实具有高度危险性的工作(如接触有毒、有害、放射性物质的岗位)才是监控的重点。对于那些没有任何危险性的一般工作岗位进行的监控,则不具有正当性。

类型三:为维护用人单位财产安全的智能监控。一般而言,该目的本身具有较明显的正当性,问题在于必要性。由于智能监控的强大数据处理能力,将其用于防止财产失窃类似于用大炮打小鸟。因而,在其他冒犯性更低的方式足以实现保护财产安全目的的情况下,应尽可能避免采取智能监控的方法。评估采取监控方式的必要性时,应综合考量是否已发生了损害事实、是否具备财产安全面临现实威胁的迹象、财产本身的价值大小等因素。例如,在一个案件中,西班牙一家超市的经理发现货架上的商品大量丢失,遂安装了监控设备,并收集到了员工偷窃货物的证据。欧洲人权法院判决认定该监控行为不违法,理由是有证据证明有违法行为和雇主重大损失的发生。^{⑤⑩}

类型四:为提升员工工作效率的智能监控。这是实践中职场智能监控的最常见目的,用人单位希望借此监督员工勤勉工作。对于那些“偷懒溜号”的员工,人工智能可将脱岗时间等相关数据记录在案,并通过算法分析作出否定性评价,甚至生成解雇的自动化决策。与前几类监控目的相比,此类监控更加具有争议性,也是社会舆论关注的焦点。在一般意义上,提升效率也具有一定正当性,毕竟企业是以营利为目的的组织。关于雇主对生产资料及其他办公资源的检查权,一些国家的立法明确予以肯定。例如,捷克《劳动法典》第316条第1款规定:“没有经过雇主的同意,雇员不能为了私人目的使用雇主为生产、服务或其他工作必需而准备的办公资源,包括计算机和其他交流技术手段等。雇主有权以适当的方式检查前述禁止性规定被遵守的情况。”但是,鉴于不间断的系统化监控对劳动者尊严的高冒犯程度,对此类监控的合法性判断应避免绝对化。除非确有十分重大的理由且没有其他更有效的提升效率手段,否则不能采取监控的手段。捷克《劳动法典》第316条第2款规定:“除非具有与雇佣活动相关的重大事由,雇主不能通过公开或隐秘的监控、电话拦截(包括记录)、查看电子邮件和邮政包裹等方式侵犯雇员在工作场所的隐私。”该款规定与第1款并不冲突,第1款中使用的“检查”(check)一

^{④⑨} 参见蒋琳:《视频监控员工违反GDPR!德国一公司被罚1040万欧元》,载网易新闻网, <https://www.163.com/dy/article/G08MSJJD05129QAF.html>, 2022年4月4日访问。

^{⑤⑩} See López Ribalda & Others v. Spain, ECtHR, Grand Chamber, Judgment of 17 October 2019[GC], apps. n.1874/13 and 8567/13.

词与第2款中使用的“监控”(surveillance)之含义并不相同。由这两款对比的体系解释可推知其立法旨意:雇主基于管理权当然有权检查其办公资源被使用的情况,但检查的手段不一定是监控,事实上,监控作为最激进的手段只在具备重大事由时才能被采用。

区分“检查”与“监控”的立场在一起雇主监督雇员网络使用状况的案件中得到充分体现。一名雇员在一个月共168小时的工作时间里,花费了102.97小时浏览与工作无关的网站,并且使用的是雇主提供的电脑。雇主获取这些信息并不是通过实时监控,而是通过事后调取查看雇员登录网站的历史记录的方式。该员工因此行为被解雇。捷克最高法院最终认定雇主的行为并未侵犯雇员的隐私,核心理由有二:第一,雇主使用的手段不是监控,而是一般化的事后检查,其冒犯性程度远低于监控;第二,雇主只是查看了雇员登录过网站的网址,以确认其是否与工作相关,但是并没有更进一步查看雇员在这些网站浏览的内容和发表的言论。^{⑤1}这一案例极好地诠释了目的原则下最小化处理的精神——监控不是人力资源管理的唯一手段,也不是首先考虑采用的手段,而应是穷尽其他方式后的最后手段。

支撑职场监控(特别是智能监控)的事由必须是重大且令人信服的,这一精神应当得到明确宣示。持续的职场监控是冒犯性极强的方式,在一些国家,秘密的职场监控甚至可能被认定为间谍行为而触发刑事责任。2021年6月,全球最大的家具零售商宜家(IKEA)就因为针对其法国员工使用间谍软件实施监控,被法国法院判处120万美元的罚金,该公司在法国的首席执行官也被判处两年缓刑及2.4万美元罚金。^{⑤2}智能监控比传统监控方式的冒犯性更强,因而只能在极少数确有必要的重大情形下例外地被采用。所谓“重大”事由,在解释上应该认为是较高门槛的要求,一般的人力资源管理需要较难构成“重大”事由。从前述列举的几种智能监控类型来看,发现犯罪、预防职业病和伤害事故等是相对较容易满足这一标准要求的情形;而为了提升效率监督员工工作表现,由于没有体现出对智能监控的紧迫性需求,且其他非冒犯性的管理手段可能也能实现这一目标,因此通常较难构成“重大”。欧盟数据保护工作组2004年发布的《通过视频监控方式处理个人数据的意见》即明确指出:“不应允许视频监控系统被用于旨在从远程位置直接控制工作活动的质量和数量,并因此进行个人信息处理。”

对我国《个人信息保护法》第13条第1款第2项所列的“实施人力资源管理所必需”是否构成足以赋予监控正当性的“重大”事由需谨慎判断。应当看到,该条款适用的对象是劳动领域一般的个人信息处理,没有更进一步具体限定到职场监控。监控比一般的职场信息处理行为更加具有冒犯性已如前述,因此适用条件的严格程度理应有所差异。在具体的法律适用中,应当在“必需”内部再区分“重大”和“非重大”,只有满足“重大”标准的人力资源管理需求才能支撑智能监控的正当性,“非重大”的管理需求则只能支撑一般的管理手段及普通个人信息处理行为。至于重大与否的判断,只能放在个案

⑤1 See Václav Šmejkal, *supra* note 48, 60–61.

⑤2 参见《宜家设计员工监控系统被罚120万美元》,载腾讯网, <https://new.qq.com/rain/a/20210618A0480E00>, 2022年4月4日访问。

中进行,以目的原则为指针,以前述类型化分析为参考。与职场监控只能例外地被采用的宗旨相悖的是,现实中的职场智能监控呈现常态化的趋势,对此需要警惕。

四、结 语

职场智能监控为数智时代背景下如何平衡个人信息利用与保护的关系提供了一个鲜活的范例。受劳动关系从属性影响,用人单位管理权和劳动者的个人信息权益形成一种特别的紧张关系,对该紧张关系的消解应以利益平衡为理念,以目的原则为进路。在用人单位管理权的制约下,劳动者的个人信息权益不得不作出一些让步。不过,管理权不能产生使劳动者个人信息权益归零的效果,即使是在工作时间和工作场所,也应认可劳动者在合理限度内的个人信息权益需得到尊重。

作为平衡之道,应基于目的原则对智能监控的范围与限度作出限制。智能监控下的劳动者个人信息处理必须具备明确、合理且与劳动直接相关的目的,在满足用人单位管理需求的同时以给劳动者造成最小损害为限度。持续性、全方位和一般预防性的智能监控应当避免,只针对工作中的敏感时段、关键场所或有迹象表明职场违法行为实施有限监控更加合理正当。鉴于智能监控与一般信息处理行为相比有更强的冒犯性,其只能作为一种例外的方式在具备重大事由时偶尔采用,不能成为常态化的管理手段,更不宜作为监视劳动者日常工作表现的常规方式。

Abstract: More and more employers begin to monitor employees with AI equipment, which threatens the rights and interests of employees' personal information more. The imbalance of algorithm power in the age of digital intelligence makes the subordination of employment relations exist and intensify with a new technical appearance, which needs to be corrected. For AI monitoring, employers and employees have legitimate and conflicting interests, and how to balance the two becomes the key. The realization of the goal of balance of interests should be centered on the implementation of the purpose principle, and the scope of AI monitoring should be demarcated. Personal information processing under AI monitoring can only be conducted with an explicit and reasonable purpose directly related to the employment and with the minimum damage to employees' interests. Employees' right to personal information should be recognized as existing in a proportionate space, even during working time and in the workplace. Continuous, comprehensive and generally preventive monitoring should be avoided, and limited monitoring should be carried out primarily for critical periods of work, key places and indications of violations of the law. In view of the highly intrusive nature of AI monitoring, it can only be exceptionally used when there are serious causes, and it can not be used as a routine means to supervise workers' performance.

(责任编辑:任彦)