Open Journal of Legal Science 法学, 2025, 13(11), 2618-2626
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.1311357

Hans汉斯

论劳动者敏感个人信息保护

李夏莹

宁波大学法学院，浙江 宁波

收稿日期：2025年10月13日；录用日期：2025年10月29日；发布日期：2025年11月21日

摘　要

敏感个人信息具备更强的算法识别性和风险损害性，立法保护也更为严格。基于劳资关系天然的对抗性、劳动者的从属性，劳动者敏感个人信息法律规制面临着告知同意原则适用失灵，法定处理前提范围过大等问题。首先明确告知同意原则和法定处理前提分别构成信息处理活动合法性评估的主客观标准，并以客观处理前提合规作为主要合法事由。结合从属性对劳动者同意的自愿性作出综合评估以弱化同意的法律效果。同时，应细化处理信息的目的，引入比例原则以有效限制法定处理前提，保证信息处理达到目的特定，手段充分必要的客观要求。

关键词

劳动者，敏感个人信息，从属性，自愿性，比例原则

On the Protection of Sensitive Personal Information of Laborers

Xiaying Li

Law School, Ningbo University, Ningbo Zhejiang

Received: October 13, 2025; accepted: October 29, 2025; published: November 21, 2025

Abstract

Sensitive personal information has stronger algorithm identification and risk damage, and legislative protection is stricter. Based on the natural antagonism of labor-management relations and the subordinate nature of workers, the legal regulation of sensitive personal information of workers faces problems such as failure to apply the principle of notification and consent, and the scope of legal processing premise is too large. On the basis of drawing on the practical experience of European information protection legislation and labor disputes, it is first clarified that the principle of consent and the statutory processing premise constitute the subjective and objective criteria for

文章引用：李夏莹. 论劳动者敏感个人信息保护[J]. 法学, 2025, 13(11): 2618-2626.
DOI: 10.12677/ojls.2025.1311357

assessing the legality of information processing activities, and the compliance of the objective processing premise should be taken as the main legal reason, and the voluntariness of the employee's consent should be comprehensively assessed in combination with the subordinate nature to weaken the legal effect of consent. At the same time, the purpose of processing information should be refined, and the principle of proportionality should be introduced to effectively limit the premise of statutory processing, so as to ensure that the information processing achieves the objective requirements that the purpose is specific and the means are sufficient and necessary.

Keywords

Laborer, Sensitive Personal Information, Subordination, Voluntariness, Proportionality

1. 引言

《中华人民共和国个人信息保护法》(下称《个人信息保护法》)的出台宣告着信息处理关系成为数字社会中重要的法律规制对象。劳动领域中，劳动者权益保护范围也因信息要素的介入相应地在发生转变，有外国学者指出雇员的隐私和个人信息是 21 世纪劳动关系最核心的问题之一[1]。《通用数据保护条例》(General Data Protection Regulation，下称 GDPR)颁布后，欧洲第二大数据侵权罚单便与劳动领域中过度收集员工信息有关：瑞典快销巨头 H&M 公司因非法对数百名员工开展监控，被德国汉堡的数据保护机构处以 3530 万欧元罚款[2]。

在我国，近几年相似的案例频繁出现：据 2019 年 4 月报道，南京市的部分环卫工人在工作时被要求带上智能手环，该智能手环能够实施监测劳动者的定位、心率等信息，当工人在原地停留 20 分钟以上，手环就会发出“加油”的提示音，鼓励其继续工作[3]。再如，据 2022 年 8 月报道，深圳某公司在每个工位上安装“一对一”监控摄像头；杭州某公司为员工购置智能坐垫，通过检测员工心跳、呼吸来确定员工是否在工位上；甚至，曾有公司采用某种行为感知系统，通过系统监测员工访问求职网站次数、简历投递的次数等具体信息考量员工的离职倾向[4]。上述案例中，用人单位通过实时监控所获取的大多是员工的医疗健康信息、行踪轨迹信息，属于《个人信息保护法》中敏感个人信息的范畴；同时，用人单位在收集相关信息后，通过自动化决策来评估员工工作表现 [1][5]。劳动者敏感个人信息权益已经面临极大损害风险。

劳动者敏感个人信息保护作为个人信息保护法领域和劳动法领域的交叉问题，是信息时代下用人单位与劳动者之间基于原有的劳资矛盾而发生的新型的权益冲突。用人单位为实现管理效率可以使用信息处理技术对员工施加监管，然而实时定位、一对一的数据跟踪和整合是否为用人单位实现“人力资源管理目标”所必须？如何理解《个人信息保护法》第 28 条第(2)款中规定的敏感个人信息的处理目的必需“特定”？上述案例中劳动者对于用人单位使用无间断的监控技术作出同意中的自愿性又应当如何评估？《个人信息保护法》第 30 条规定的在告知同意框架下的单独同意原则在劳动领域能否具体适用？本文从劳动者敏感个人信息的概念和特征出发，结合相关司法案例，重点探讨敏感个人信息处理规则在劳动领域适用的具体困境，对保护劳动者敏感个人信息权益提出相应的规制建议。

[1]最常见于外卖骑手等网约工的工作模式。

2. 劳动者敏感个人信息的界定

2.1. 敏感个人信息的一般界定

《个人信息保护法》采用“概括 + 列举”的方式对敏感个人信息的概念和类型作了基本的界定，[2]然而这种界定方式也会给敏感个人信息保护范围带有不确定性[6]，因此有必要厘清敏感个人信息与一般个人信息、私密信息的区别，这对界定敏感个人信息的合理范围有重要意义。

第一，敏感个人信息区别于私密信息，私密信息更多强调信息的私密性，落入隐私权的法定范围，[3]保护的是信息主体不愿被打扰的私生活安宁。敏感个人信息更强调与算法的结合度，可计算性更强。曾有学者认为个人信息是一种独特的生产要素和经济资源，因其具备线上的可计算性而产生财产价值[7]。诸如行踪轨迹、生物识别信息的出现和广泛应用正是植根于强大的信息采集和处理技术，[4]因此敏感个人信息更加注重与信息主体以及其他信息的关联性。比如人脸信息并不具备私密性，但与信息主体的财产信息却高度关联。反之，信息主体的性取向的信息属于典型的个人私密信息，此种信息显然也不必以信息技术为依托而存在，却非常注重保密功能。强调两者不同意味着传统的隐私权救济路径无法完全保障现在的信息主体合法权益[8]。

第二，敏感个人信息区别于一般个人信息，有学者认为其敏感性体现在法律规制的反应度更高，而这种高反应度源于敏感个人信息的权益损害风险更高[9]。敏感个人信息风险损害性更强的主要表现在于一方面，这种高风险性也表现为风险形式也从传统的被识别转向被歧视、被控制的风险形式转变和扩散；另一方面其指向的权益更为复杂，具体表现为：一是诸如人脸识别信息等敏感信息到信息主体更为重要的财产利益；二是特定领域的权益也将遭受侵害，比如消费者因大数据杀熟技术获得“私人报价”，其知悉真情权、公平交易权等消费权利被同时侵害；劳动者可能面临就业平等权被侵害等问题。三是信息侵害不仅涉及到私主体合法利益保护，也牵扯到维持数据生态、数据信任等公共利益保护[10]。

2.2. 劳动者敏感个人信息的特殊性

劳动者敏感个人信息保护问题在法律规制上有一定的特殊性，具体体现包括三个方面：一是侵犯的信息类型和数量，劳动是个人主要的社会活动，用人单位采集信息类型包括教育履历、家庭背景、职业经历、健康状况、工作能力、兴趣爱好等[11]，组合而成的是一个人较为完整的身份数据画像。二是侵犯信息的时间和空间范围。相比于消费关系，劳动关系具有持续性，劳动者敏感个人信息可能在求职、工作、离职等各阶段出现[12]；三是侵权损害后果更为严重。劳动者敏感个人信息不仅关乎个人隐私，更直接关联其就业平等权、职业健康等基本权益。再者，劳动作为一项基本权利，劳动者信息权益相比于消费者信息权益的更为重要，牵扯到更为直接的机会平等问题。

劳动者敏感个人信息的特殊性既反映出原有的劳资矛盾问题，也折射出信息时代独有的社会矛盾。曾有学者已经指出信息处理关系本身也作为一种不平等的关系，与劳动关系同样具有合作性与对抗性[13]，随着信息处理技术成本进一步降低，信息利用保护这一矛盾使得原有的劳资矛盾有了新的转型。合作关系体现为信息互通与共享：通过线上信息传播流通，资源置换和管理能够消除不必要的信息壁垒，从而更为

[2]《个人信息保护法》第 28 条第 1 款规定：“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。”

[3]参见《民法典》第 1032 条第 2 款。

[4]如今，通过监控技术能够快速抓拍交通违法行为、通过人脸识别技术能够识别定位犯罪份子侦破重要刑事案件；生活中，我们凭人脸快速出入高铁站检票口，通过佩戴智能手表准确监测我们的健康数据和实时位置，这些都曾是我们无法预料的技术福音。

有效地实现经济价值和管理目标。[5]因此，用人单位处理劳动者敏感个人信息具有一定正当性与必要性。

然而，双方关系具有天然的对抗性，劳动者在劳资关系中处于天然的从属性地位。不同的经济技术背景之下，用人单位为追求私欲而尝试采取不同形式的榨取劳动力价值的方式。数字社会下这种对于劳动者控制、压迫的方式也变得更为隐蔽化、柔性化，从而造成对劳动者权益更大的威胁和破坏趋势。职场监控为典型的例子。用人单位基于更强大的监控技术和算法权力对劳动者实施全方位的监控，有学者提出了数字时代下的劳动者的第四种从属性——“技术从属性”[14]，折射出了劳动关系的对抗性在数字经济下的新变化：居家办公成为新的办公形式；短视频博主通过创作来获得平台的打赏；骑手、网约车司机能够自由支配上下线时间。劳动者看似逐渐脱离了原有的人身控制，但这种“来去自由”[15]的背后是信息、技术等新型的经济资源和生产要素向资方逐渐聚集和靠拢，资本增值能力不减反增[16]。劳动者仍然“一无所有”，从属性地位没有发生改变。因此我们更应避免劳动者落入形式自由的禁锢之中，加强劳动者敏感个人信息的保护十分紧要。

3. 劳动者敏感个人信息保护的立法困境

在《个人信息保护法》出台前，关于敏感个人信息的保护规定分散在各类法律和行业规范中，缺乏系统性。该法确立了敏感个人信息的重要地位，并对其处理规则作出专章规定。然而，针对劳动领域的信息处理活动，立法仍显不足。现行条款仅在一般信息处理的合法性基础中提及用工场景，[6]但是在适用于敏感个人信息处理活动时需要作进一步限制处理。其中，“为实施人力资源管理所必需”这一表述存在外延不清的问题，而“必需”又具有语境依赖性，需要更为细化的规定来规制职场中典型的信息处理场景才能得以落实。相较之下，《劳动合同法》第 8 条虽限制用人单位在招聘阶段收集与合同相关的信息，却未规定后续处理方式和安全保障义务，也难以覆盖工作期间及离职后的信息处理，存在明显空白。

以下将重点探讨告知同意原则框架下“单独同意”原则(第 29 条)的适用困境，以及敏感信息处理的法定前提(第 28 条第 2 款)在劳动领域中的具体适用问题。

3.1. 告知同意原则在劳动领域下适用失灵

“告知–同意”原则是全球范围内通用的信息处理的黄金规则。《德国黑森州信息法》作为欧洲的第一部个人信息保护的立法，便已经将告知同意原则作为个人信息收集原则予以确定[17]。《通用数据保护条例》(GDPR)中，同意也是信息处理重要的合法性基础之一，并且规定对于特殊数据的处理要获得信息主体明确的同意。近年来，告知同意原则在信息处理活动中所存在的漏洞也被许多学者所诟病，以告知同意原则不可作为所有信息收集行为的合格抗辩，要受目的原则与必要原则的限制。有学者认为告知属于兼具公法及私法性质的行为，而同意属于私主体对自己个人信息权益的处分，基于此提出要构建“同意撤回”制度[18]。劳动领域下，有学者指出同意的内在困境在劳动者个人信息处理中更为鲜明[19]；也有指出劳动者信息保护的特殊性，知情同意原则在资强劳弱的背景下适用失灵的问题。

3.1.1. 告知义务流于形式：知情的充分性不足

根据“告知–同意”原则，劳动者作出同意的前提是充分知情，因此用人单位负有告知信息处理活动的法定义务。关键在于：告知义务的具体要求为何？劳动者知情的范围应如何界定？

《个人信息保护法》第 17 条规定了告知义务的形式与实质要求，第 31 条进一步明确，处理敏感个

[5]比如，区别原有传统线下的填写信息表、咨询谈话等收集信息的形式，如今企业可以通过在线加密文档等形式收集员工信息，并基于算法对信息做进一步的分类整合，有利于对员工的个性管理。

[6]《个人信息保护法》第 13 条第 2 款规定：“为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需。”

人信息时须告知处理的必要性及对个人权益的影响，标准更为严格，有助于缓解告知流于形式的问题。[7]但是，该条款仍然存在一定细化的空间，比如这里的“必要性”是否可以和第 28 条第 2 款法定处理前提中“充分的必要性”有冲突？“必要性”应当作何解释？

此外，信息在不同处理阶段均具价值。用人单位收集信息后可能进行多重利用，如人脸识别信息既用于考勤，也可用于监控工作状态或结合算法评估绩效。若用人单位以模糊、笼统方式告知，掩盖真实处理目的，劳动者将难以察觉。因此，有学者认为，“单独同意”原则应配套“单独告知”，避免一揽子式告知[20]。

另一方面，劳动者普遍缺乏对敏感个人信息权益的认知，难以理解信息与其人格、财产利益的关联，以及信息处理可能带来的具体风险。而用人单位未必客观告知相关影响，因此有必要引入第三方评估机制，判断信息处理目的是否特定、正当。此外，不应将理解复杂政策的负担完全归于劳动者，并让其承担由此产生的不利后果。

3.1.2. 单独同意缺乏自愿性

我国《个人信息保护法》第 29 条规定的“单独同意”原则，在“告知–同意”框架下对同意提出了更高要求。“单独”意味着非概括性授权，体现法律对信息主体自决权的重视。但劳动者处于从属地位，其同意往往难以真正自愿，同意的效力存疑。此时，强调“单独”形式反而可能掩盖核心问题——即劳动者缺乏拒绝用人单位的现实能力。用人单位常以管理目的为由要求提供信息，劳动者即便知情也难以拒绝。而同意一旦成为处理敏感信息的合法性基础，就可能被企业用作规避法律责任的工具，带来重大合规隐患。因此，劳动者同意能否作为合法事由值得质疑。

曾有学者基于这种困境，提出将员工的集体同意又或是劳动规章下的集体合意作为同意的替代性适用，立法趋势也显示出对集体合意的倾向。[8]然而，现实中集体协商的真实性仍难保障。比如，2021 年，北京某用人单位曾以员工手册的规定要求员工提供完整病例，否则不允许批假，[9]法院最终认定侵犯隐私权，反映出规章制度中劳动者权益易被虚置。尽管同年七部门联合发文赋予劳动者和工会对涉及自身权益的规则提出协商意见的权利，但实际操作中，劳动者对敏感信息处理的认知不足、协商机制不健全，导致权利行使受限。

综上，劳动领域中的“告知–同意”原则面临适用困境：告知流于形式，同意缺乏保障。

3.2. 处理的法定前提有待限制

《个人信息保护法》第 28 条第 2 款规定，处理敏感个人信息须具备特定目的、充分必要性并采取严格保护措施，标准更为严苛。但在劳动场景中，“特定目的”如何界定、何为“充分必要”仍不明确，需围绕目的过度扩张和手段必要性缺乏限制两方面进一步细化。

3.2.1. 处理目的有待特定化、正当化

合法、正当、必要和诚信原则已成为个人信息处理的基本原则，[10]而敏感信息处理还需目的“特定”。

[7]一般信息处理的告知要求对于告知的实质内容未作细化规定。目前，许多数字经济体采用加粗、划线等清晰的方式提醒用户，然而告知内容仍然十分冗长和专业化，用户仍然无法提出实质性抗衡的异议，因此告知行为仍然只是在形式上完成了立法的要求，仍然给了信息处理者过大的规避空间。

[8]宪法和法律委员会曾对《个人信息保护法》草案三次审议稿中关于第 13 条处理信息的合法性基础中的“为人力资源管理所必需”作出必要限制，并修改为“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”，《个人信息保护法》现行立法采纳了这一观点。参见全国人民代表大会宪法和法律委员会关于《中华人民共和国个人信息保护法(草案三次审议稿)》修改意见的报告，载中国人大网 2021 年 08 月 20 日，http://www.npc.gov.cn/npc/c30834/202108/5e507c650c4147f6a600d9935868b2c5.shtml。

[9]一审判决部分支持了该员工的诉讼请求，二审判决维持了一审判决结果，再审驳回该用人单位的再审申请。参见达科信息科技(北京)有限公司与谢涛劳动争议案，北京市朝阳区人民法院(2019)京 0105 民初 63471 号民事判决书、北京市第三中级人民法院(2021)京 03 民初 106 号民事判决书、北京市高级人民法院(2021)京民申 3957 号裁定书。

[10]参见《个人信息保护法》第 5 条。

有学者指出，目的正当性是更高层次的要求，只有目的明确、特定，才可能认定其正当[21]。但当前立法对“特定”缺乏具体解释，用人单位处理目的的正当边界亦不清晰。

首先，对于“特定”缺乏具体理解和落实。结合个人信息法中第 17 条所规定的，用人单位在将劳动者信息用于不同的“处理目的”时要重新获得主体同意。若对“处理目的”仅作宽泛理解，用人单位获取员工行踪轨迹、人脸识别等敏感信息后，可将其用于考勤、监控工作时间、评估绩效等多重用途，均被笼统归入“人力资源管理”范畴，从而获得极大抗辩空间。这不仅导致告知义务流于形式，也削弱了合法性审查的有效性。因此，应结合“单独同意”原则，将“特定”理解为具体、非概括的目的。在劳动领域，处理目的必须场景化，不得以提升管理效率等抽象理由作为合法性基础。唯有目的具体化，才能判断其是否服务于用人单位的正当利益(即目的正当性)，进而评估处理手段是否充分必要。

其次，第 13 条第 2 款将“实现人力资源管理所必需”限定于劳资协商前提下，试图通过集体同意约束目的范围。曾有学者指出“国家主导”摸下的集体协商将指标管理作为核心策略，这导致了实践中地方政府和工会围绕指标提高集体合同数量，集体协商的本质从劳资博弈发展为地方机关联合工会与资方的讨价还价行为[22]。在此背景下，“集体同意”反而可能使正当目的边界被扩大，进一步增加劳动者信息被滥用的风险。

3.2.2. 充分必要性难以落实

第 28 条第 2 款要求处理敏感个人信息须具备“充分的必要性”。尽管信息流通有助于提升效率，劳动者也应合理让渡部分信息权益，但该让渡必须以“充分必要”为限。职场监控是典型例证：其既涉及劳动者敏感信息，也体现用人单位通过技术手段维护财产、行使管理权的新形式。关键在于，如何公平界定信息处理范围与劳动者权益保护的边界。司法实践中，法院往往优先考虑经济效率，倾向于支持用人单位。例如，2018 年南京某单位在宿舍对面安装摄像头，法院以未拍摄隐私内容或公开影像为由，认定无实质性损害，驳回员工诉求。[11]2019 年山东某单位在员工电脑安装监控软件，法院认为出于正当利益且仅用于举证，未造成实质伤害，未支持劳动者主张。[12]

再如考勤制度，部分企业为防止代打卡而使用指纹或人脸识别等敏感信息，这种高强度方式的必要性值得质疑。[13]在非传统用工场景下，是否确有必要通过如此高强度手段实现管理目的？持续监控易引发心理不适，削弱劳动者的主体性，甚至导致精神压力或疾病。同样，在病假管理中，单位核实健康状况可理解，但并无必要获取全部病历。信息收集应依据目的与影响程度进行比例评估。可见，“充分必要性”在实践中落实困难，现行法律未能有效平衡管理需求与劳动者权益保护，导致信息处理手段易被滥用，亟需立法进一步细化适用标准。

4. 劳动者敏感个人信息保护之建议

4.1. 告知同意原则的优化

4.1.1. 明确告知同意原则与法定处理前提的关系

告知同意原则侧重劳动者主观意愿，而法定处理前提(如特定目的、充分必要性、严格保护措施)则提供客观判断标准。鉴于劳动者在劳动关系中的从属性，其敏感信息保护应以事前客观评估为主、事后救济为辅，以法定处理前提为核心，告知同意为补充。

[11]王雅云与中国石化集团金陵石油化工有限责任公司隐私权纠纷案，参见江苏省南京市栖霞区人民法院(2018)苏 0113 民 1926 号民事判决书。

[12]该案历经一审、二审阶段，一审驳回修某全部诉讼请求，二审维持一审判决。参见修玉婵、海阳市融昌塑编包装有限公司隐私权纠纷案，山东省海阳市烟台市人民法院(2019)鲁 0687 民初 224 号民事判决书、山东省烟台市人民法院(2019)鲁 06 民初 7145 号民事判决书。

[13]现实中，也有针对人脸识别发生的劳动争议。参见江苏省苏州市中级人民法院(2021)苏 05 民初 6603 号民事判决书。

劳动者的从属性决定了其同意难以真正自愿。过度强调同意，可能引发两种极端：一是劳动者过度控制信息，导致信息闭塞，影响用人单位为提升管理效率或提供福利(如保险、住宿、个性化管理)所必需的信息处理；另一个极端便是同意可能再次异化。即使对于同意原则作出限制，比如，将其限制下集体同意之下或是同意基础劳资协商程序产生，事实上，德国联邦数据法第 26 条第 4 款中也有相应的规定。正如前述，这种做法值得商榷。基于我国目前的劳资协商机制的发展现状以及工会机构与用人单位的力量对比的情况来说，集体同意仍然无法解决员工的自愿性缺乏的问题，仍难保障劳动者真实意愿，反而可能掩盖个体诉求。

同意原则陷入悖论，正因其在缺乏合法性基础时仍被广泛用作“帝王条款”，成为企业规避责任的工具。因此，应弱化其在劳动领域的适用效力：劳动者同意因非完全自愿，其法律证明力应相应减弱。用人单位即便获得同意，也须以符合法定处理前提作为必要补充；若无法提供其他合法性依据，仅凭同意难以在争议中免责。

告知同意原则是用人单位处理劳动者敏感信息的重要原则，但并非唯一的处理规则。鉴于其主观性与真实性不足，应将法定处理前提作为限制性、优先性原则，在适用位阶上高于同意原则。从立法体系看，《个人信息保护法》第 28 条第 2 款(法定前提)位于第 29 条(单独同意)之前，也体现了立法者对二者关系的制度安排。

4.1.2. 从属性作为同意自愿性司法审查的重要因素

在借鉴德国《联邦数据条例》第 26 条第 2 款的基础上，应当引入“原则无效，例外有效”的评估方式，在综合全面考量员工的从属性地位后作出对同意的自愿性的司法判断。审查的核心为衡量员工是否具有自由选择性，例外情况可以包括：

一是雇员在经济上或者法律上存在积极利益的情况，可以认定自愿性：比如说公司为员工安排旅游，为员工提供购买优惠的医疗保险又或是其他商业保险等福利产品时需要员工的银行账号或者是身份证号等等，公司为员工提供优惠的住宿需要员工的身份识别信息。

二是雇员可能与雇主存在利益诉求一致的情况，比如员工代表公司参加竞赛、又或是员工参与单位的抽奖或评比活动等等。对于利益诉求一致的情况，用人单位也有权收集员工信息，因为员工对于竞赛、评比等活动有不参加的权利。

三是双方利益诉求并不一致的情况下，如果单位采取了保护措施，并为员工能够提供选择余地的情况也应考虑在内例外情况范围之内。上述列举情况均可以成为实务中衡量自愿性时的参考，司法实践中也可以进一步总结自愿性的例外情况。

4.2. 法定处理前提的具体限制

用人单位滥用同意原则处理劳动者敏感信息的原因之一便在于法定处理前提没有得到具体的落实和限制。因此，有必要借鉴相关经验，对目的“特定”，手段“必要充分”作出限制性规定。

4.2.1. 处理目的特定化、场景化

审查用人单位处理敏感信息的前提是目的必须具体、明确。可结合《个人信息保护法》对用工场景下合法基础的规定，在立法层面进一步细化。例如，“为订立、履行合同所必要”可扩大解释至离职阶段，并细化为合同订立、履行及离职三个阶段的具体目的。

第一，合同订立阶段。包括了解劳动者学习、工作能力及健康状况等。例如，对特定岗位(如护理、服务业)确需了解健康信息的，可作适度限定。同时，犯罪记录作为典型敏感信息，应主要通过隐私权路

径救济，[14]这一点值得肯定，因为犯罪记录更为反应的是信息的私密性，信息主体不愿透露的主观意愿，但若用人单位利用前科信息进行算法分析，则应纳入个人信息保护的规制范围。

第二，工作阶段中“为人力资源管理所必要”的处理目的，可以进一步拆解为防范性骚扰等职场违法行为，为提供有人身、财产安全的办公场所，代员工缴纳社保、医疗保险，考察员工出勤情况；监管员工的工作情况、考核其工作业绩等等。这些都是立法上可以规定的重点场景和重要处理信息的目的。司法上，法院可以通过颁布司法解释的方式具体解释用人单位处理信息的目的以避免笼统、概括、不明确的处理目的。比如，用人单位可以采用职场监控技术，必须是基于合法、正当的目的，比如可以为了防范职场性骚扰等行为来进行一定的职场监控。

4.2.2. 比例原则的具体适用

比例原则要求用人单位在具备正当、合法、特定的处理目的，还要采用能够满足目的并对劳动者权益损害最小的信息处理方式。

从信息类型看，若一般信息足以实现目的，不得收集敏感信息。例如，为考勤管理目的，采用指纹、人脸识别并不必要，也存在较高风险，用 ID 卡或 NFC 识别即可满足需求。再如，若仅为考核工作表现，不应通过监控技术长期记录员工行为或如厕次数，否则违反比例原则与职场伦理。

从信息数量上来说，如果必需收集敏感个人信息，信息处理数量范围必需以处理信息目的为限。比如，医疗健康数据是法定的敏感个人信息，前述的修某请假案中用人单位收集的关于修某生病的健康信息应当仅限于能够正面刚修某生病的结论性意见，而并不能收集修某的全部病例信息，属于过度收集，违反了比例原则。再比如，用人单位如果出于防治职场中的违法行为采取视频监控，监控的信息内容也必须以目的原则为限，不得长时间、持续地对员工进行监控，同时监控信息应当在一定期间被销毁。

5. 结语

劳动者敏感个人信息保护体现出用人单位与劳动者在信息时代下基于原有的劳资矛盾而发生的新型利益冲突。敏感个人信息具备更高的算法识别性和风险损害性，立法保护更为严格。劳动领域下，工作场所、工作设备日益数字化，信息处理与利用矛盾的介入使得原有的劳资矛盾加剧，劳动者更大程度地被监控、分析、控制，劳动从属性地位加剧。告知同意原则中同意的自愿性无法充分实现，必需综合考虑劳动者从属性因素来评估同意的自愿性的效力，并弱化同意在劳动领域下的具体适用。与此同时，将个人信息保护法第 28 条第(2)款的法定处理前提作为主要合法事由，并围绕目的特定、手段充分必要，严格保护措施形成信息处理合法性评估的客观标准。最后，引入比例原则，实现信息处理手段与处理目的的相适应。针对劳动领域中招聘面试、职场监控等重点保护场景，有待立法和司法解释出台细化规则。

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(3): 25-39.

[2] 白一方, 周颖. 违法收集员工信息零售巨头 H&M 被罚 3500 万欧元[EB/OL]. https://www.fx361.com/page/2021/0315/7768194.shtml, 2021-03-15.

[3] 为扫街环卫工配发“手环”引争议[N]. 劳动报, 2019-04-11(005).

[4] 张丽. 职场“监视”花样多 员工隐私易泄露“防摸鱼”与方便管理的边界在哪[N]. 法治日报, 2022-08-13(004).

[5] 赖祐萱. 外卖骑手, 困在系统里[J]. 人物, 2020(8): 70-91.

[6] 王苑. 敏感个人信息的概念界定与要素判断——以《个人信息保护法》第 28 条为中心[J]. 环球法律评论, 2022, 44(2): 85-99.

[14]福州市榕桥物业管理有限公司、陈林学劳动合同纠纷案，福建省福州市中级人民法院(2019)闽 01 民终第 4020 号民事判决书。

[7] 彭诚信. 数字法学的前提性命题与核心范式[J]. 中国法学, 2023(1): 85-106.
[8] 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.
[9] 宁园. 敏感个人信息的法律基准与范畴界定——以《个人信息保护法》第 28 条第 1 款为中心[J]. 比较法研究, 2021(5): 33-49.
[10] 丁晓东. 个人信息公私法融合保护的多维解读[J]. 法治研究, 2022(5): 14-25.
[11] 王倩. 作为劳动基准的个人信息保护[J]. 中外法学, 2022, 34(1): 183-201.
[12] 谢增毅. 职场个人信息处理的规制重点——基于劳动关系的不同阶段[J]. 法学, 2021(10): 167-180.
[13] 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[J]. 中外法学, 2022, 34(2): 445-464.
[14] 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.
[15] 张恂. 数字经济时代资本主义劳资关系的新样态及本质透视——基于马克思“资本-劳动”二元对立关系的分析框架[J]. 思想教育研究, 2023(1): 76-82.
[16] 徐景一. 算法机器与资本控制: 劳动过程理论视域下的平台劳资关系与资本积累[J]. 社会主义研究, 2022(3): 32.
[17] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
[18] 万方. 个人信息处理中的“同意”与“同意撤回” [J]. 中国法学, 2021(1): 167-188.
[19] 吴文芳. 劳动者个人信息处理中同意的适用与限制[J]. 中国法学, 2022(1): 221-243.
[20] 韩旭至. 敏感个人信息处理的告知同意[J]. 地方立法研究, 2022, 7(3): 67-82.
[21] 刘权. 论个人信息处理的合法、正当、必要原则[J]. 法学家, 2021(5): 1-15+191.
[22] 吴清军. 集体协商与“国家主导”下的劳动关系治理——指标管理的策略与实践[J]. 社会学研究, 2012, 27(3): 66-89+243.