

作为劳动基准的个人信息保护

王 倩*

摘 要 劳动者的个人信息保护问题存在特殊之处,具体表现为资强劳弱和人格从属性背景下知情同意规则的失灵、工作数字化后劳动者被透视和被操控的风险、有组织生产的合作关系中个人信息处理的需要,因此不能完全适用《个人信息保护法》的一般规则。劳动基准法已经纳入立法规划,在其中就劳动者个人信息保护做专门规定,这是对数字时代人权保护新挑战的回应,对于其他劳动基准的实现也有重要意义。在劳动关系中仅遵循私法路径不足以保护个人信息,还需要配备公权力保障,劳动基准法的双重保护机制也契合了这一需求。作为劳动关系中保护个人信息的特别法,劳动基准法的相应条款应该考虑如何对一般规则进行调整,包括限制知情同意规则的适用,满足人力资源管理的正当需求,修改删除权、可携带权和自动化决策条款,协调主管机构、救济方式和法律责任。由于“必需”是一个语境依赖型概念,将来还应该通过配套文件来规制工作场所的视频监控等典型的应用场景。

关键词 劳动基准法 个人信息保护 数字化 人力资源管理

据 2019 年 4 月初报道,作为“智能环卫”项目的一部分,南京市的部分环卫工人被要求在上班时佩戴用人单位配发的一款智能手环,该智能手环具备实时定位、监控心率、一键呼叫等功能,可以显示环卫工人是否按时出勤、有无脱离工作区域,而且只要环卫工人上班时在原地停留 20 分钟,就会自动发出“加油”的语音提示他继续工作,相关数据都会上传到单位,成为奖惩的依据。部分环卫工人对此并不理解,认为无法避免出勤不出力,用人单位则称此举有利于及时了解工人的工作状况,还能通过综合调度指挥,迅速派人抵达目标地点清理垃圾,既降低了管理成本,也提升了城市清洁的效率。^[1] 从劳动者的个人信息保护角度来看“智能手环监

* 同济大学法学院副教授。本文系国家社会科学基金一般项目“数字化时代劳动者的个人信息保护研究”(项目编号:20BFX190)的成果。

[1] 参见熊颖琪:《环卫工智能手环监工功能引争议,环卫公司:已取消》,载新华网,http://www.xinhuanet.com/local/2019-04/05/c_1124330252.htm,最后访问日期:2021 年 12 月 17 日。

工”事件,用人单位使用智能手环实时监控劳动者,处理了多种劳动者个人信息,其中至少涉及健康信息、行踪轨迹两项敏感个人信息,由系统基于收集的信息判断劳动者的出勤情况、工作效率并做出奖惩,涉及自动化决策。那么,劳动者在领取智能手环时签署的一揽子知情同意书是否有效,之后能否以“非自愿”来抗辩?监控心率、收集行踪轨迹是否为实施人力资源管理所必需,用人单位降低成本、提高效率的理由成立吗?劳动者对于奖惩结论有异议的怎么维权,是否能以用人单位严重侵犯其个人信息权益为由辞职并主张经济补偿金?用人单位涉嫌侵犯劳动者个人信息权益的,应该是网信部门还是劳动监察部门来处理?

我国《个人信息保护法》已经于2021年8月20日出台,上述部分问题已经有了答案,部分问题却并未得到解决,还需要进一步立法完善。由于劳动者的个人信息保护问题存在特殊之处,不能完全适用一般规则,短期内修改《个人信息保护法》的可能性不大,加入大量特别规定还会妨害原本的规制体系和框架,更为合适的路径是在劳动法领域设置特别法。虽然《劳动合同法》第8条规定,用人单位招用劳动者时有权了解劳动者与劳动合同直接相关的基本情况,但是部分观点认为该规定仅适用于订立劳动合同的环节,^{〔2〕}而且只是限定了用人单位可以处理的劳动者个人信息的范围,离完善的劳动者个人信息保护机制还很远。^{〔3〕}劳动基准法已经纳入十三届全国人大常委会立法规划,可以考虑在其中就劳动者个人信息保护做专门规定。据报道,中国人民大学版的《劳动基准法专家建议稿》在总则中明确了劳动者的隐私与个人信息受法律保护,^{〔4〕}但可惜只有一条简单的原则性规定,难以解决前述问题。需说明的是,本文并不认为劳动基准法是“具有公法性质的、以保障劳工权益为主旨的国家与雇主间权利义务关系的基本法”,^{〔5〕}而是采“劳动基准法是保护劳动者利益的强行性法律规范的总合”之学说,包含私法性劳动基准法、公法性劳动基准法和双重效力劳动基准法。^{〔6〕}劳动者的个人信息权益受到侵害的,既可以通过主管行政部门的责令改正、罚款等方式予以救济,也可以通过劳动仲裁、诉讼的程序来维权。

一、劳动者个人信息保护的特殊之处

《个人信息保护法》直接涉及劳动关系的仅有第13条第1款第2项,即“为订立、履行个人

〔2〕 参见全国人大常委会法制工作委员会行政法室:《最新中华人民共和国劳动合同法解读与案例》,人民出版社2013年版,第85页。

〔3〕 另有《就业服务和就业管理规定》第13条要求用人单位对劳动者的个人资料予以保密,公开劳动者的个人资料信息须经劳动者本人书面同意,不过该部委规章的规定层级较低,在理论界和实务界也从未受到过重视。参见王锡铤、彭鏊:“个人信息保护法律体系的宪法基础”,《清华法学》2021年第3期,第21页。

〔4〕 参见张菁:《〈劳动基准法〉专家建议稿(中国人民大学版)研讨会成功举办》,载中工网,http://right.workercn.cn/34164/202107/21/210721131825282.shtml,最后访问日期:2021年12月17日。

〔5〕 林丰宝、刘邦栋:《劳动基准法论》,三民书局2018年版,第9页。

〔6〕 参见沈建峰:“劳动基准法的范畴、规范结构与私法效力”,《法学研究》2021年第2期,第76—94页。

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”的,可处理个人信息。相对于该法草案的一审稿、二审稿完全不考虑劳动关系框架下个人信息保护的的特殊性,最终定稿对用人单位处理劳动者个人信息的合法性基础做了特殊安排,是一种明显进步,却还是留下了较大的规制空间。劳动关系中的个人信息保护与一般语境下的个人信息保护相比较,主要有以下不同。

(一)资强劳弱和人格从属性背景下知情同意规则的失灵

《民法典》第 1035 条第 1 款基本上把信息主体的知情同意视为合法处理个人信息的前提,^{〔7〕}《个人信息保护法》第 13 条第 1 款虽然列举了七种处理个人信息的合法性基础,却也是将“取得个人的同意”列在第 1 项。然而,在劳动关系中适用《个人信息保护法》第 14 条及以下条款的知情同意规则却存在较大困难。单个劳动者相对于用人单位在信息、财力、技术等各方面事实上处于弱势地位,劳动关系的核心特征又是人格从属性,即劳动者在工作时间、工作地点、工作内容和履行方式等方面听从于用人单位的指挥,融入了用人单位的组织之中。个人信息的种类、利用方式和途径非常复杂,原本普通用户就不大可能花费大量的时间精力去阅读企业不断更新的、复杂、冗长而专业的隐私政策,也缺乏理解相关条款的知识储备和能力,对于个人信息被侵犯造成的危险后果认识也有限。^{〔8〕}在劳动关系中大量、持续进行个人信息处理的背景下,劳动者同样缺乏时间、精力及能力去了解情况,有时甚至难以察觉其个人信息处理的发生,无法达到充分知情的要求。

更为重要的是,普通用户还有可能因为个人信息保护方面的顾虑而放弃使用或者选择其他应用程序,而应聘者在激烈的就业市场中则不太可能为此牺牲工作机会,甚至可能为了获得竞争优势而主动公开相关信息。在职劳动者为了避免冲突、保住岗位,即使预知到了个人信息权益被侵犯的风险,在用人单位收集处理其个人信息时大多采取服从管理、听从安排的态度,^{〔9〕}比如在实践中有相当多的用人单位在考勤管理中使用人脸识别技术,却鲜有劳动者敢于反对刷脸打卡,甚至在诉讼中用人单位将刷脸记录作为证据提交时,法院也很少质疑使用人脸这一高度敏感的生物识别信息进行考勤管理的正当性和必要性。^{〔10〕}所以,事实上和法律上的弱势地位导致劳动者难以真正自由地、自愿地进行选择。反之,若劳动关系中个人信息保护得不到落实,又会导致用人单位对劳动者的监督和控制更加肆无忌惮,从而导致进一步的人

〔7〕 最高人民法院民法典贯彻实施工作领导小组主编:《中华人民共和国民法典人格权编理解与适用》,人民法院出版社 2020 年版,第 376 页。

〔8〕 参见丁晓东:《个人信息保护原理与实践》,法律出版社 2021 年版,第 90—91 页。

〔9〕 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”,《比较法研究》2021 年第 3 期,第 34 页。

〔10〕 参见辽宁省沈阳市中级人民法院(2021)辽 01 民终 12398 号民事判决书、江苏省苏州市中级人民法院(2021)苏 05 民终 6603 号民事判决书、贵州省六盘水市中级人民法院(2021)黔 02 民终 2705 号民事判决书。

身依附和地位悬殊。

(二)工作数字化后劳动者被透视和被操控的风险

劳动关系中个人信息暴露得彻底和全面,需要防止用人单位对劳动者的“透视”。劳动者日常生活的大部分时间都在工作场所度过,即使在私人时间的活动也可能直接或间接地与工作相关,劳动关系中用人单位原本就会持续获得大量的劳动者个人信息,而劳动世界的日益数字化^[11]更是加剧了这一状况。工作中智能手机、平板电脑、手持式扫描仪、可穿戴设备等的使用逐渐普及,在公司 OA 系统、微信群、在线办公平台等内部和外部沟通平台上的活动也日益频繁。劳动者每天在工作时使用这些软硬件的过程,伴随着大量的个人信息的收集、使用、加工、传输等各种处理。通常某个应用程序收集到的应该是用户与使用该程序相关的特定方面的个人信息,比如某打车软件收集到某个用户用车的频率和喜好、行踪轨迹、支付账户等信息。相比之下,劳动合同从缔结、履行到解除或终止的过程中,用人单位收集和处理的个人数据种类更多、更全面,可能反映劳动者职业经历、工作表现、医疗健康、社会活动、金融账户、家庭情况、兴趣爱好等不同方面的个人信息,将相关数据组合起来进行综合分析更容易形成人格画像,劳动者在用人单位面前更为透明。

在数字化的工作过程中,用人单位可以收集到海量的个人信息,配合以相应的算法,智能化的管理系统可以飞速地进行分析、关联、预测、判断、反馈,而自动化决策的过程往往又是频繁而隐蔽的,劳动者难以应对、甚至无法觉察,用人单位却容易“抽身事外”,可以号称系统不会出错,但在发生争议时把责任推卸给算法。如此一来,劳动者可能沦落为被系统、算法操控的对象,《个人信息保护法》的规定却更多地面向消费者保护的场景。比如第 24 条第 2 款要求“通过自动化决策方式向他人进行信息推送、商业营销,应当同时提供不针对其个人特征的选项,或者向个人提供便捷的拒绝方式”,主要是为了解决“信息茧房”、大数据杀熟等问题,在劳动关系中难以适用。劳动关系中出现的场景则更多是招聘单位使用简历自动筛选系统过滤掉不合适的候选人、用人单位应用智能管理系统对劳动者进行考核奖惩、在此基础上做出“不胜任工作”的调岗或解雇决定等,这些自动化决策直接影响到劳动者安身立命的“饭碗”,而第 24 条第 3 款所规定的要求予以说明的权利、拒绝自动化决策的权利对此恐怕作用有限。

(三)有组织生产的合作关系中个人信息处理的需要

一般语境下,个人信息保护主要是解决信息主体的权益保护和信息业者或国家机关对信息的开发利用之间的矛盾。然而,劳动关系中的用人单位并非信息业者,不是直接利用劳动者的个人信息营利,也不像国家机关那样是为了维护公共利益、履行法定职责而处理个人信息,其角色更多是介于信息业者与国家机关之间。用人单位处理个人信息是为了提高工作效率、确保服务质量、保护人身和财产安全、维持营业场所秩序、履行社保缴纳义务和合规要求等目的,与之相冲突的是劳动者的隐私保护、安全健康、劳动报酬、平等就业等各种权益。

[11] 参见田思路:“智能化劳动管理与劳动者隐私权的法律保护”,《湖湘论坛》2019 年第 2 期,第 17 页。

用人单位是生产经营的组织者,要维持这个组织体的正常有序运转,在此过程中要分配工作任务、发出指令,监督劳动者是否适当履行任务和服从指令,辅之以相应的奖惩,^[12]在对劳动力资源进行配置调度的过程中,必然要对劳动力所有者的个人信息进行处理。劳动合同又是典型的继续性合同,存续时间往往比较长,且期间不断产生给付义务和附随义务,双方之间有较强的信赖关系。^[13]用人单位对于劳动者负有各种照顾义务,同时负有各种社会责任,在履行义务和承担责任的过程中也不可避免地要处理劳动者的个人信息。制度设计必须考虑到这些特征和需求,比如,劳动关系中的个人信息处理是在不同场景下大量地、持续地进行的,如果每次、每个人都要进行告知同意,信息处理目的、方式等发生变更的还要重复,会让双方疲于应付,也导致效率低下,而入职时的一揽子、概括性同意又不能满足法律对处理敏感个人信息等特殊行为的特殊要求,所以很有必要将“人力资源管理所必需”设置为个人信息处理的合法性基础。个人信息也有社会流通属性,^[14]用人单位这个“小社会”内部并非一般的陌生人场域,其中的社会交往和信息流通更为频繁密切,赋予劳动者过多的控制权并不合适。比如,公司制作的内部通讯录中包含了员工的姓名、所属部门、职务职级、工作电话和邮箱等信息,如果认为此举属于个人信息处理者公开其处理的个人信息从而需要取得员工的单独同意,显然是荒谬的,但是将前述信息公布在公众可以随意访问的公司官网上,就要区分员工是否从事负责对外联络的工作等具体情况了。

二、个人信息保护作为劳动基准的必要性

(一)数字化时代人权保护的挑战

劳动基准法最重要的功能在于保障劳动者的基本人权,传统的劳动基准主要涉及劳动者的生命安全、身体健康以及劳动者生存所依赖的劳动报酬待遇等。^[15]然而,随着移动互联网、大数据、云计算、人工智能等科技迅猛发展,人类进入数字化时代,数据的产生呈现爆炸式增长,数据的处理速度和能力大幅提升、成本大幅下降,数据成为至关重要的资源,人们的社会行为和日常交往都在不断地数字化。人权形态正在经历着深刻的数字化重塑:一方面,人权保护面临着全新的威胁和侵蚀,无限制的、全面扩张的监控使得个人可能随时随地被监督和检视,黑箱算法不仅能做出预测、还可用于控制个人的行为,导致各种歧视和不公;另一方面,新

[12] 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”,《法学》2021年第2期,第163页。

[13] Vgl. Gaier in: Münchener Kommentar zum BGB, 8. Aufl., 2019, § 314 BGB Rn. 6.

[14] 联邦宪法法院在著名的1983年12月15日的“人口普查案”中指出,个人信息自决权并非个人对其个人信息享有的绝对的、不受限制的控制权,人是在社会中生存发展的,需要与其他人交流沟通,vgl. BVerfG NJW 1984, 419 (422).

[15] 参见《劳动与社会保障法学》编写组:《劳动与社会保障法学》,高等教育出版社2017年版,第191页。

兴数据和信息权利正在理论和制度层面、国内和国际范围、私法和公法领域逐步获得确认和保护,大大丰富了生存权、发展权的时代内涵,开启了以“数字人权”为代表的“第四代人权”。^[16]

具体到劳动关系中,人权保护同样面临着结构性的变化。应聘面试被问及婚育家庭情况、入职前安排体检、工作场所安装视频监控等现象仍然普遍存在,但是工作设备、工作过程和工作对象的日益数字化带来了新的风险,前述“智能手环监工”事件便是典型例证。可以说,数字化社会中个人信息保护和利用的矛盾冲突在劳动用工的场景下表现得更为明显,用人单位几乎是每时每刻在进行着对劳动者的个人信息处理,随之而来的是劳动关系中愈发多见的隐私侵犯、歧视对待、全面监控、行为操纵等现象。

然而,劳动者不是机器,需要尊重信任和自由空间,不能允许用人单位用高科技给劳动者带上镣铐,我国《宪法》第38条所规定的对公民人格尊严的保障需要在各种法律关系中得以落实。《个人信息保护法》第1条开篇明义地指出是“根据宪法,制定本法”,《民法典》最大的创新和亮点是人格权独立成编,加大了对隐私权和个人信息的保护力度,^[17]第四期国家人权行动计划还专设了一节,强调要加强个人信息保护、完善有关法律制度。^[18]所以,我们也不能停留在保障肉体生存的层面上来理解劳动基准,精神性的利益保护愈发重要,关乎人格尊严和自由发展的个人信息保护应成为劳动基准法的内容,否则就是自动放弃劳动法的发展空间。实际上,劳动基准法的内容在历史上也呈现出一个逐渐扩展的过程,^[19]立法较早的日本、韩国的《劳动基准法》中没有涉及个人信息保护,英国的劳动基准法则包含了劳动者的个人信息保护制度,^[20]波兰和匈牙利的《劳动法典》也在近期修订时增加了多个有关个人信息保护的条款。^[21]

(二)对其他劳动基准实现的意义

用人单位掌握着大量的劳动者个人信息,可以运用先进的数据处理技术在此基础上利用算法做出决策,除了可能导致就业歧视,^[22]自动化决策还会影响到劳动者休息休假、劳动报酬、职业安全等各方面的劳动条件。曾经刷屏的“外卖骑手,困在系统里”报道中提到,某外卖平台使用的“实时智能配送系统”会将骑手的潜能和速度挖掘到最大限度,同一距离的外卖订单最长配送时间被不停地缩短,配送时间和准时率又和配送费挂钩,骑手们为了准时送达违反交通规则也在所不惜,从而导致事故频发。^[23]工厂里也有类似场景:据报道某电子设备制造

[16] 参见马长山:“智慧社会背景下的第四代人权及其保障”,《中国法学》2019年第5期,第6、13页。

[17] 参见王利明:“民法典人格权编的亮点与创新”,《中国法学》2020年第4期,第5—25页。

[18] 参见常健:“既往开来的第四期国家人权行动计划”,载《人民日报》2021年9月13日,第16版。

[19] 参见王全兴:《劳动法》,法律出版社2017年版,第67页。

[20] 参见闫冬:“英国劳动基准立法”,《中国劳动》2012年第12期,第33页。

[21] 参见谢增毅,见前注[9],第37页。

[22] 就业歧视问题不是本文关注的焦点,就此另有学者研究,参见阎天:“女性就业中的算法歧视:缘起、挑战与应对”,《妇女研究论丛》2021年第5期,第64—72页。

[23] 参见赖祐萱:“外卖骑手,困在系统里”,《人物》2020年第8期,第71—74页。

公司引入了智能员工管理系统,遍布车间的摄像头、车间门口的电子考勤系统和录入所有工人信息的 OA 系统分工合作,几乎替代甚至超越了原来车间主管的工作:摄像头负责监控所有工人的在岗情况和工作效率,系统会通过画面识别工人动作,用录像记录下每个人加工元件的时长并与规定时间比对;电子考勤系统把打卡程序细化到车间,工人离开岗位超过规定时间也会被提交到 OA 系统;OA 系统把摄像头录像和考勤记录归档,每月根据工人的工作量和缺勤情况进行绩效考核,缺勤和效率低下者会被扣工资,超额完成者则受到额外奖励。虽然公司允许员工对考核结果提出异议,但即使上级进行人工复核,一般还是采信 OA 系统的判断。比如某次工人去洗手间的时间超出规定 3 秒就被系统扣了工资,车间主管帮其申诉后,上级仍然维持了系统的决定。^[24]

可见,如果任由用人单位使用智能系统对劳动者进行全方面监控,运用算法技术分析收集到的个人信息,再配合以相应的考核、奖惩来引导操控劳动者的行为,可能导致劳动强度不断增加、休息时间难以得到保证、劳动报酬受到影响等后果。劳动者不可能一直保持高效,人类监督下还有“喘息”机会,系统却看得一清二楚,算法还可能把这种状态作为标准,持续提出“优化”工作表现的要求。“提高工作效率”“监督员工出勤”可以是用人单位处理劳动者个人信息的正当理由,但是将这种目标追求推向极致,会导致对于剩余价值的残酷压榨。长期来看,剥夺劳动者的自主空间对用人单位也未必是好事,因为异化为“工具”的劳动者是缺乏能动性和创造力的。此外,现实生活中纷繁复杂的因素并非都能转换成机器可读的数据和程序,系统是依据冰冷且一成不变的计算逻辑做出决策,而人类又是具备反思能力、拥有七情六欲的主体,其行为也不是完全可预测。^[25]虽然自动化决策也可能出现错误判断,算法却看上去客观又中立,用人单位更容易推卸责任,劳动者往往难以反驳,只能被动接受。无怪乎欧盟委员会在 2020 年 2 月 19 日公布的《人工智能白皮书》中强调,在招聘过程中或者在影响劳动者权利的情况下使用人工智能应用的,应该视为高风险活动,将来设计监管框架时有必要确定强制性法律要求。^[26]严格监管的机制之一就是加强劳动者个人信息保护,因为从源头上看,劳动者的个人信息是用人单位进行算法管理的“原材料”;从结果上看,用人单位又是针对性地将算法运用在劳动者个体身上,所以规制用人单位对劳动者个人信息的处理,也是预防用人单位利用算法过度“压榨”劳动者的重要路径,关系到其他劳动基准的保障。

(三)私法、公法双重规制的必要

个人信息私法保护的作用不容忽视。^[27]《民法典》第 1034 条及以下条款对个人信息保

[24] 参见刘畅:《我的领导不是人》,载微信号“财经 E 法”,2021 年 1 月 11 日上传。

[25] 参见(英)凯伦·杨、马丁·洛奇:《驯服算法》,林少伟、唐林垚译,上海人民出版社 2020 年版,第 28—30 页。

[26] See European Commission, *White Paper on Artificial Intelligence-an European approach to excellence and trust*, p. 18, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf, last visited on 17 December 2021.

[27] 参见程啸:“民法典编纂视野下的个人信息保护”,《中国法学》2019 年第 4 期,第 26—43 页。

护的规定体现了立法者对个人信息私法保护的高度重视,劳动者作为自然人也享有《民法典》赋予的民事权益。《个人信息保护法》更进一步在第四章赋予了个人在个人信息处理活动中的知情决定权、查阅复制权、更正补充权、删除权等权利;而且根据第 50 条,个人信息处理者拒绝个人行使权利的请求的,个人可以依法向人民法院提起诉讼。前述规定并未将劳动关系排除在适用范围之外,劳动者可以向用人单位主张这些权利,而将来明确这些规范属于劳动基准,重点在于强调它是保护性强行法,不能被当事人的意思所排除,构成保障劳动者权益的底线,^[28]比如用人单位让劳动者签署承诺书放弃个人信息保护的相关权利或者通过合同约定减轻或排除自己作为信息处理者的义务和责任等行为无效,但是劳动合同或集体合同中可以作出更有利于劳动者的约定。^[29]

然而,仅在私法上进行权益界定和保护不足以完全解决问题,尤其在主体地位不平等、持续时间长、又强调信赖合作的劳动关系中,还需要借助公法的保护机制,即设置国家的监督、强制和惩罚,才能提供更为充分、全面和有效的个人信息保护。^[30]之所以在劳动关系中实现个人信息保护需要配备公权力保障,主要因为以下几方面的原因:

第一,实践中指望劳动者来主张《民法典》或《个人信息保护法》所赋予的权利可能性不大,尤其是在劳动关系的存续期间,劳动者缺乏主动维权的能力、精力和动力,却直接面对着不听从用人单位命令就会被处罚、甚至解雇的风险,侵害发生之时不敢反抗,事后维权又存在着举证困难、赔偿有限等种种障碍;相反,行政监管可以在侵害发生之时就介入,甚至之前就发挥警示预防等作用,执法效率也更高。这并非否定私法保护路径,只是它经常是在劳动关系没有成功建立或者劳动关系结束之后才发挥作用。第二,劳动合同的顺利履行有赖于双方之间的信赖与和平,充斥着提防和猜忌的工作氛围必然是有害的,借助公权力实现个人信息保护有利于促进劳资双方的信任和合作;反之,劳动者提起仲裁或诉讼主张权利往往意味着和用人单位“撕破脸”,可能影响到劳动关系的稳定和谐。^[31]比如,德国联邦议会曾经在 2010 年讨论过专门的《雇员个人信息保护法草案》,立法理由中就特地强调了该立法对于创设“充满信任的工作氛围”的重要意义。^[32]第三,劳动关系具有很强的外部性,劳动关系中的个人信息处理经常是大规模、持续性发生,关涉到公共利益和秩序,应该配置公法效力。虽然目前我国劳动监察的力量较弱、资源缺乏,甚至有各种行政不作为的情形,却并非不可改变的状况,而且网信、

[28] 参见沈建峰,见前注[6],第 80 页。

[29] 比如,虽然欧盟《通用数据保护条例》第 88 条规定,成员国可以通过法律或通过集体协议制定特定规则以确保在雇佣语境下处理雇员个人数据时保护其权利和自由,但是集体合同或者企业协议的约定不能突破条例的底线,即只能在条例所赋予的个人信息保护上“做加法”。Vgl. Pauly in: Paal/ Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 3. Aufl., 2021, DS-GVO Art. 88, Rn. 4.

[30] 参见王锡锌:“个人信息国家保护义务及其展开”,《中国法学》2021 年第 1 期,第 145—166 页。

[31] 就是否应该配备公权力保障需要考虑的因素,参见沈建峰,见前注[6],第 82—83 页。

[32] Vgl. Deutscher Bundestag 17. Wahlperiode, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, Drucksache 17/4230.

公安、市场监督管理等部门也有监管职责,将来还可以设立专门、独立、权威的个人信息保护执法机构,^[33]只要做好部门之间的权责划分和配合衔接,避免相互推诿即可。

三、劳动基准法中保护个人信息的特殊安排

对于在劳动关系框架下保护个人信息没有什么特殊之处的事项,在劳动基准法中重复一遍《个人信息保护法》的规则没有多大意义,用好援引技术就能解决问题。更重要的是基于劳动关系的特殊性,考虑需要进行哪些调整。所谓调整既不是因为劳动者的弱势地位而一味加强保护,也不是为了回应用用人单位人力资源管理的需要而整体降低标准,而是针对性地部分强化、部分弱化。此外,还需要在实体规则、程序安排和机构设置方面做好两部法律的衔接。

(一)主体上的适用范围设定

作为劳动基准的个人信息保护机制不应该严格地以存在劳动关系为适用前提,而应该吸收域外法经验采取功能性的定位,即权利主体不应该局限于劳动者。欧盟的《通用数据保护条例》第 88 条针对的是“雇佣语境下的处理”,强调“在如下情形中尤其适用:为了招聘,履行劳动合同,履行法律或集体合同规定的义务;对工作的管理、计划和组织;工作场所的平等与多样性;工作中的健康和 safety;对员工和顾客财产的保护;为了行使和履行与雇佣相关的权利和义务;为了终止雇佣关系。”该规定重视的是事实状态和保护需求,而不是法律上的分类。^[34]德国立法者更是直接在顺应条例修改后的《联邦数据保护法》第 26 条第 8 款中表明,该法意义上的雇员不仅包括劳动者,还包括学徒工、参加残疾人就业促进项目的人、类雇员、公务员等群体;该法不仅适用于劳动关系存续期间,也适用于劳动合同缔约前和结束后的相关个人信息处理。其保护范围不可谓不广。有学者特别指出该法保护类雇员意义重大:平台经济的从业者是否属于劳动者目前仍有争议,但是他们基本都对平台有经济从属性且需要倾斜保护,所以至少能够认定为类雇员,平台用工每天都在发生大量的从业者个人信息处理,急需相关条款的调整。^[35]

不管是在招录阶段为了签订劳动合同进行磋商,还是在劳动合同解除或终止之后处理后续的相关问题,应聘者与招聘单位之间、前员工与前用人单位之间都存在着类似合同的信赖关系,产生处理个人信息的需求也基本源于即将成立劳动关系或曾经有过劳动关系,所以应该适用同样的个人信息保护机制。招聘单位出于招录员工的目的处理求职者的个人信息,比如收集审核简历、要求提交各种材料、面试时询问各种问题、安排体检等,都是容易出现个人信息保护问题的典型场景,实践中也出现了招聘单位使用简历自动筛选系统、委托第三方对候选人进

[33] 参见周汉华:“个人信息保护的法定定位”,《法商研究》2020年第3期,第52页。

[34] Vgl. Riesenhuber in: BeckOK DatenschutzR, 36. Ed. 1.2.2021, DS-GVO Art. 88 Rn. 30.

[35] Vgl. Däubler, Gläserne Belegschaft, 9. Aufl., 2021, S. 154.

行背景调查等新情况。在劳动关系结束之后,一方面,劳动关系存续期间已经收集的个人信息还存在着再次处理的问题,比如前用人单位能否向第三方透露劳动者在职期间的奖惩情况,形成所谓的“职场黑名单”?另一方面,用人单位还有可能为了履行离职竞业限制约定的支付义务和通知义务、支付企业补充养老保险待遇等,需要继续收集处理前员工的个人信息。

更为重要的是,我国庭审实践中认定劳动关系大多适用的是原劳社部 2005 年 5 月 25 日发布的《关于确立劳动关系有关事项的通知》,往往要求劳动者“主体适格”,所以一直以来大学生兼职、实习、退休人员或超龄人员再就业等认定劳动关系存在困难,但是在用工过程中一样存在着个人信息处理的问题。另外,平台经济近年来发展迅猛,目前我国有数千万计的网约车司机、外卖配送员等依托互联网平台就业,组织型平台中的部分劳务提供者可以相对自主地决定是否工作、何时以及何地工作,平台对劳动过程的控制也与传统的劳动管理有所不同,导致平台与劳务提供者之间的法律关系定性争议很大。^[36]因此,假设我们只给予与用人单位有劳动关系的劳动者以个人信息保护,那么上述群体大多会被排除在适用范围之外,虽然他们在个人信息保护的事实状态和保护需求上和劳动者没有本质区别,与用工主体之间同样存在着持续的、不平等的信息处理的关系。实际上,由于上述平台从业人员往往工作时间和地点灵活机动,平台不能像传统用人单位那样“在眼皮底下”进行管理,所以反而会为了达到监督控制的目的收集更多信息。比如,外卖平台实时监控骑手配送过程中的具体位置和运动轨迹,骑手的到店时间、取餐时间、送达时间等都一清二楚,还可以通过用户评价或投诉得知骑手的服务态度等表现。^[37]就平台从业人员的基本劳动权益保护,人社部等 2021 年 7 月 16 日发布的《关于维护新就业形态劳动者劳动保障权益的指导意见》已经做出了表率。该意见首次提出了“不完全符合确立劳动关系情形”的表述,即不完全符合确立劳动关系情形但企业对劳动者进行劳动管理的,以后要将此类就业人员纳入“最低工资和支付保障、休息和劳动定额、劳动安全卫生责任”等制度的覆盖范围内。这些正是劳动基准制度的核心内容,将来新就业形态的劳动者权益保障也应该包含个人信息保护。

另外,义务主体方面应该考虑设置小微企业和个体工商户的豁免条款。持续不平等的信息关系应该是个人信息权利保护的适用前提,即无论是从思想资源、制度框架起源,还是从欧美等域外法的规定来看,个人信息权利保护针对的对象都是具有专业性或商业性信息收集特征的主体,尤其是利用现代科技大规模收集个人信息的主体。^[38]我国现行劳动法没有对小

[36] 参见王玉:“互联网平台用工的类雇员解释路径及其规范体系”,《环球法律评论》2020 年第 3 期,第 86 页。

[37] 参见赖祐萱,见前注[23],第 71—91 页。

[38] 参见丁晓东:“个人信息权利的反思与重塑:论个人信息保护的适用前提与法益基础”,《中外法学》2020 年第 2 期,第 342—344 页。比如美国《加州消费者隐私法》将受管辖的企业范围限定于年收入超过 2500 万美元的公司,或为了商业目的而收集、出售或共享 50000 条以上个人信息的公司,又或年收入的 50% 以上为销售消费者个人信息所得的公司。

微企业和个体工商户的优惠待遇,然而如果对所有的用人单位一刀切地适用个人信息保护的规定,可能导致保护目的的落空或法律争议的泛滥。一方面,小微企业和个体工商户用工人数不多,处理的个人信息有限,数字化技术和设备也不是很普及,老板与员工之间的强弱对比不是那么明显,人身信任关系却更强,相应造成的个人信息保护的风险和可能的威胁也没那么大。另一方面,小微企业和个体工商户规模小、资金少,往往缺乏个人信息保护方面的专业人才、知识和意识,而过高的合规成本和保护标准可能导致其财务负担和经营困难。^[39]实际上,《个人信息保护法》的立法者也意识到了执行该法对小微企业可能造成的负担,所以在第62条规定国家网信部门要针对小型个人信息处理者制定专门的个人信息保护规则标准。

(二)“知情同意”规则适用的限制

由于劳动关系中往往缺乏真正的知情基础上的自主选择、自由决定,大多数情况下用人单位不能基于劳动者的同意进行个人信息处理。当然,这并不意味着在劳动关系框架下,劳动者的同意绝对不能单独作为用人单位处理其个人信息的合法性基础。欧盟的《通用数据保护条例》草案曾经规定,在数据控制者和数据主体之间存在着“明显不平等”的地位时同意无效,但是最后的定稿放弃了此立场,反而是在“鉴于条款”第155条提出,应该由成员国法律或集体合同来设立雇佣语境下基于雇员同意而进行的数据处理规则。^[40]因此,德国《联邦数据保护法》第26条第2款规定,判断同意是否自由做出,需要特别考虑劳动关系中劳动者的从属性以及表示同意时的具体情形,但是在劳动者可以获得法律上或经济上的好处时或者在用人单位与劳动者的利益诉求一致时,可认为同意是自由做出的。欧盟数据保护委员会也认为,在一些特殊情况下,企业可能证明同意的自愿性,比如企业请某办公区域的员工在以该区域为背景的电影或视频中出镜,但不愿意被拍摄的员工不会受到任何形式的惩罚,可以在拍摄期间在其他区域获得相同的办公空间。^[41]我国劳动基准法立法可以借鉴此经验,规定原则上只有在劳动者可以获得法律上或经济上的好处时,或者在用人单位与劳动者的利益诉求一致时,用人单位可以基于劳动者的同意处理其个人信息,用人单位能证明劳动者的同意是自愿做出的除外。

由于《个人信息保护法》第13条第1款第2项、第3项和第4项都有“所必需”的要求,第5项和第6项有“在合理的范围内”的限制,而第1项没有这样的表述,所以作为劳动基准的个人信息保护尤其要强调,即使劳动者的同意是充分知情、自愿、明确的,用人单位基于劳动者的同意处理其个人信息还是要受到正当必要原则、目的限制和最小化原

[39] 参见谢增毅:“劳动法与小企业的优惠待遇”,《法学研究》2010年第2期,第99—101页。

[40] Däubler, a.a.O., S. 135.

[41] EDPB, *Guidelines 05/2020 on consent under Regulation 2016/679*, p. 9, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf, last visited on 17 December 2021. 就GDPR下处理员工个人数据的合法性基础问题,参见王倩、顾雪莹:“GDPR下涉欧企业的员工个人数据合规管理”,《德国研究》2021年第2期,第121—125页。

则、公开透明原则等各种限制。^{〔42〕}以面试场景为例,即使应聘者的同意有效,招聘单位的知情权也受到限制:^{〔43〕}一方面,从“宽度”上看,其收集处理的信息应该与考察应聘者是否具备从事该工作的资质和能力相关,比如不得在面试时询问应聘者是未婚还是已婚、打算生几个小孩;另一方面,从“深度”上看,即使招聘单位收集处理的信息与从事该工作直接相关,也不能构成对应聘者人格尊严过分的、不恰当的压迫和干涉,比如不得对应聘者进行压力测试、声音分析或者面部微表情识别。

另外,《个人信息保护法》第23条、第25条、第26条、第29条、第39条分别规定,个人信息处理者向其他个人信息处理者提供其处理的个人信息的、公开其处理的个人信息的、将所收集的个人信息或身份识别信息用于维护公共安全的目的之外的其他目的时、处理敏感个人信息时、向境外提供个人信息的,需“取得个人的单独同意”。实践中有观点误以为上述个人信息处理活动都只能以个人的单独同意作为合法性基础,^{〔44〕}忽略了《个人信息保护法》第13条第2款的表述。“单独同意”只是对同意的升级,有第13条第1款第2项到第7项情形的,不需要取得个人同意,自然也不需要单独同意,将来劳动基准法中也应该明确这一点。实际上,单独同意的要求在劳动关系中能够发挥的保护效果有限,虽然相对于概括的、一揽子的同意能够起到明确警醒、提示风险的作用,但一般情况下还是不能解决劳动者“不敢说不”的问题;而在特殊情况下劳动者与用人单位发生矛盾的,又可能被劳动者当作对抗用人单位的武器,妨碍正常的用工管理。比如劳动者有较大的收受商业回扣嫌疑时,拒绝用人单位为调查目的收集其金融账户信息。

(三)人力资源管理需求的满足

由于在大多数情况下劳动者的同意不能作为用人单位处理其个人信息的合法性基础,所以《个人信息保护法》第13条第1款第2项的规定对于劳动关系中的个人信息处理至关重要。在该法的立法过程中,“一审稿”和“二审稿”并无相关表述,二次审议之后有委员、专家指出企业、单位在人力资源管理工作中需要处理个人信息,建议在草案中补充此情形,从而“三审稿”中增加了“或者人力资源管理所必需”;就此又有常委委员提出需对该规定进行必要限制,^{〔45〕}所以最后的定稿变成了“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

〔42〕 参见张新宝:“个人信息收集:告知同意原则适用的限制”,《比较法研究》2019年第6期,第1—20页。

〔43〕 参见王倩:“招聘阶段用人单位知情权的限制:也谈《劳动合同法》第八条后半句的理解和适用”,载林嘉主编:《社会法评论》(第5卷),中国人民大学出版社2011年版,第85—104页。

〔44〕 参见劳动观察:《〈个人信息保护法〉实施在即,HR不得不知的15大要点!》,载劳动报, <https://www.51ldb.com/shsldb/zc/content/017b70ee6fd2c0010000df844d7e124a.html>,最后访问日期:2021年12月17日。

〔45〕 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)》审议结果的报告”和“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”,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572—575页。

管理所必需”。〔46〕

可见,由于立法者认为“订立或履行劳动合同所必需”不能完全覆盖劳动用工场景下的需求,所以增加了“实施人力资源管理所必需”这一独立的合法性基础。此举是务实的,《个人信息保护法》没有像欧盟《通用数据保护条例》第6条第1项那样把“为了追求数据控制者或者第三方正当利益之必要”作为合法性基础,所以必须有相应补充。严格从字面意义上看,订立或履行劳动合同并不包括解除或终止劳动合同,然而实践中此环节用人单位必然要处理劳动者个人信息,比如适用《劳动合同法》第40条第2项进行“不胜任解雇”的,要用到大量关于劳动者工作表现、绩效考核、培训或调岗的信息;之后发生劳动争议的,也不可避免要在劳动仲裁、诉讼中使用其作为证据。还有一些人力资源管理的场景与劳动合同本身没有直接关系,比如公司为员工购买福利性质的补充医疗保险、提供员工宿舍进行管理、追究离职员工侵犯商业秘密的责任,需要收集相关信息。然而,用人单位很可能会利用其优势地位扩大解释“人力资源管理所必需”,立法者正是意识到了该路径被滥用的可能性,所以尝试用集体层面上职工利益代表的博弈来弥补不足。

虽然从逻辑上讲,人力资源管理的需求能够覆盖所有与劳动合同相关的情况,但是此时用人单位未必有“依法制定的规章制度”或“依法签订的集体合同”作为依据,而这一限制又是不可或缺的。所以,将来劳动基准法中应该将“为订立、履行、解除或终止劳动合同所必需”与“按照依法制定的劳动规章制度或依法签订的集体合同实施人力资源管理所必需”作为两种并列的、相互独立的合法性基础予以列举。就《个人信息保护法》第13条第3至第7项所列举的其他几个合法性基础而言,其涉及情形未必与前述两项相重合,在劳动关系下的适用又没有多少特殊之处,所以劳动基准法直接援引即可。

不过,至少短期内不能对于劳资协商或民主程序起到的制约作用期待过高。〔47〕由于我国基层工会在组建设置、人员选任、经费来源等方面往往依赖于资方,尚未真正成为劳动者的集体利益代表,各地的集体协商大多以行政化手段推行,存在着严重的指标化、数字化和形式化,部分集体合同存在内容空洞、流于形式的问题。〔48〕对于劳动规章制度,虽然法律要求需经民主协商程序制定,但是只要求听取职工意见,最后还是由用人单位拍板确定,容易出现“走

〔46〕 此处法律表述上可能有一个不妥之处需要纠正,规章制度与集体合同在制定主体、程序要求、内容事项、法律效力等各方面都有区别,分属两种不同的劳动关系调整机制,有其一作为依据即可,所以应该是“或”,而非“和”。

〔47〕 德国《联邦数据保护法》第26条第1款所规定的数据处理合法性基础,除了有“建立、履行或终止劳动关系所必需”之外,也包括“行使或履行基于法律、集体合同或企业协议产生的权利义务所必需”。不过这也是以德国强大的集体协商、劳资共决机制作为支撑的,比如联邦劳动法院早在1984年9月14日的判决中就认为,雇主引入电脑信息系统处理雇员工作行为与业绩的,属于《企业组织法》第87条第1款第6项的情形,需要得到企业职工委员会的同意,vgl. BAG, NZA 1985, 28(29).

〔48〕 参见常凯:“劳动关系的集体化转型与政府劳工政策的完善”,《中国社会科学》2013年第6期,第101页。

“过场”的现象,部分裁判意见甚至并不否定未经民主程序的规章制度的效力。^[49] 所以,司法实践中还是要对个人信息的处理是否属于实施人力资源管理所必需进行实质性审查。比如在“达科信息科技(北京)有限公司与谢某劳动争议”中,劳动者以“抑郁状态”为由向达科公司申请病假并提交了病体的诊断证明书,之后用人单位以《员工手册》等规章制度为依据要求其提供完整病历、心理治疗凭证、心理治疗单据、医药费凭据、心理治疗材料、精神分析治疗材料;劳动者拒绝提供后,用人单位以旷工为由将其解雇。法院认为,劳动者提交的诊断证明书已经能够反映其存在抑郁状态且有建议休息的医嘱,其罹患疾病的细节应属个人隐私;用人单位要求提供的病历、心理证明材料、费用凭据等应以必要为限,能够反映患病就诊事实即可,不应过分求全,以免侵犯个人隐私,侵害患者权益。^[50]

(四)“必需”的具体化与典型问题的规制

判断是否“为订立、履行、解除或终止劳动合同所必需”“按照依法制定的劳动规章制度或依法签订的集体合同实施人力资源管理所必需”,会是将来保护劳动者个人信息的核心问题。欧盟数据保护委员会对《通用数据保护条例》第 6 条第 b 项“履行合同所必需”的解释持相当谨慎的态度,需从合同目的出发基于事实判断是否存在客观上的必要、是否符合数据主体的合理期待、是否有对其权益影响较小的替代选择。^[51] 德国立法者提出,在理解《联邦数据保护法》第 26 条第 1 款的“建立、履行或终止劳动关系所必需”时,应在雇主与雇员相互冲突的基本权利间寻求一致性,尽可能在雇主处理数据的正当利益和雇员的人格权益之间达成平衡。^[52] 德国联邦劳动法院则在众多判决中根据比例原则进行了必要性审查,即首先看雇主处理雇员的个人信息是否有助于目的的达成,然后看是否存在更温和的、对雇员权益侵害更轻的手段,最后再看雇主追求的目的与对雇员权益的影响是否相称时进行利益衡量。^[53] 可见,界定“必需”是个难题,因为它一个典型的“语境依赖型”概念。^[54]

然而,仅通过劳动仲裁或法院在个案中的裁判意见起到的救济效果和示范作用有限,行政

[49] 参见《广东省高级人民法院、广东省劳动争议仲裁委员会关于适用〈劳动争议调解仲裁法〉、〈劳动合同法〉若干问题的指导意见》(粤高法发[2008]13号)第 20 条。

[50] 由于该案审结时《个人信息保护法》还没有出台,所以法院援引的法条依据为《民法典》第 1034 条,参见北京市第三中级人民法院(2021)京 03 民终 106 号民事判决书。

[51] EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, pp. 9-10, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art-6-1-b-adopted_after_public_consultation_en.pdf, last visited on 17 December 2021.

[52] Vgl. Deutscher Bundestag 18. Wahlperiode, Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, Drucksache 18/11325.

[53] Wybitul, Der neue Beschäftigtendatenschutz nach § 26 BDSG und Art. 88 DSGVO, NZA 2017, 413(415); BAG, NZA 2017, 394(396).

[54] 参见(荷)玛农·奥斯特芬:《数据的边界》,曹博译,上海人民出版社 2020 年版,第 168 页。

机关、裁审部门需要更加清晰的规则依据,用人单位和劳动者也需要更为明确的行为指引。考虑到劳动者个人信息保护的应用场景多样、科学技术和社会经济环境的发展变化迅速,^[55]而法律又需要保证一定的抽象性和稳定性,所以劳动者个人信息保护的典型场景不适合直接由劳动基准法本身进行规制,而是应该放在劳动基准法的配套性文件中处理。将来可以针对入职面试与体检、背景调查与职场黑名单、工作场所的视频监控、电话监听和局域网监控、行踪轨迹与生物识别信息的处理等实践中最普遍的、冲突最明显的问题,由人力资源和社会保障部出台专门的部门规章,配合以最高人民法院定期公布的劳动人事争议典型案例,从而兼顾确定性与灵活性的需要。

以工作场所的视频监控为例,《个人信息保护法》第26条调整的是为了维护公共安全在公共场所安装视频监控设备的行为。然而,除展览厅、体育场、银行窗口、酒店大堂、超市售货区等部分工作场所同时构成公共场所以外,^[56]更多工作场所是公众不能自由进出的,用人单位安装视频监控可能是为了防止公司财产偷盗和商业秘密泄露、维持生产流程和经营秩序、监控劳动者的工作表现、预防和制止违纪行为等目的。工作场所的视频监控又可能对劳动者的人格尊严和自由产生较大威胁,因为镜头下劳动者的一举一动都可能成为被观察、记录和分析的对象,包括完成工作时的行为、与同事和上司的交流、甚至当时的姿态和表情,容易造成很大的精神压力,劳动者不免战战兢兢、行为受限。^[57]虽然工作场所并非私人空间,劳动者的举动本来就可能被别人所打量,但是人能够获得的信息有限,没有视频监控这种“上帝视角”和强大的保存、复制、分析的功能。如何处理视频监控场景下劳动者的个人信息保护问题?将来可以考虑形成以下规则:第一,工作场所进行视频监控应该是出于保障人身和财产安全、维持生产经营秩序、确保工作义务履行、防止违法犯罪行为等正当目的;第二,对于更衣室、卫生间、淋浴房、休息室等私密区域不得进行视频监控;第三,原则上视频监控应公开进行,设置显著的提示标识,除非为了调查具体的违法犯罪行为不得不进行秘密监控;第四,不得为了监督控制劳动者的工作表现而对其进行长时间不间断的监控,出于其他目的不得不进行的持续监控也不得用于评判劳动者的工作表现;第五,应该尽量使用更为温和的视频监控技术,实时监控能够达到目的则不得进行录像,需要录像的保存期限应为实现处理目的所必要的最短时间且应及时删除。^[58]

[55] 比如上世纪九十年代学者在讨论劳动者在工作场所通信的问题时,除了谈到电子邮件还涉及了书面信件和传真,但是现在后两种通信方式已经很少使用了,参见张新宝:“雇员在工作场所的隐私权保护与限制”,《现代法学》1996年第5期,第6页。

[56] 关于公共场所的界定问题,参见龙卫球主编:《中华人民共和国个人信息保护法释义》,中国法制出版社2021年版,第112—114页。

[57] Vgl. Riesenhuber, in: BeckOK DatenschutzR/, 37. Ed. 1.2.2021, BDSG § 26 Rn. 144.

[58] 德国联邦劳动法院曾经面临类似的难题,在系列判决中总结了一些规则可供借鉴,vgl. BAG, NZA 2003, 1193(1195); BAG, NJW 2005, 313(315); BAG, NZA 2008, 1187(1191); BAG, NZA 2018, 1329(1332).

(五)删除权、可携带权与自动化决策条款的修改

《个人信息保护法》第47条的规定在劳动关系中适用可能面临困境。部分情况下会有多种信息处理的合法性基础可供选择,比如用人单位处理劳动者的医疗健康信息、请假记录等,虽然也为计算医疗期、发放病假工资等人力资源管理所必需,但是开始时用人单位可能选择了基于劳动者同意而进行个人信息处理。如果之后劳动者和用人单位间产生矛盾,比如就是否应该批准病假有争议,那么劳动者可能会撤回同意;此时按照第47条第1款第3项,用人单位有义务删除相关信息,未主动删除的,劳动者有权请求删除。然而,劳动关系中往往需要保证处理个人信息的连续性和完整性,比如用人单位按照《劳动合同法》第40条第1项解除劳动合同的前提条件之一是劳动者患病且法定医疗期届满,判断医疗期是否届满需要有前后完整的记录,如果由于劳动者撤回同意而删除之前的信息,就算之后的信息处理用人单位还能援引其他的合法性基础,仍然会使得用人单位难以进行病假管理,“因病解雇”导致仲裁、诉讼时也会无法举证。相比之下,欧盟《通用数据保护条例》第17条第1款第b项的规定更为周延,即“数据主体撤回同意且没有其他数据处理的合法性基础的情况下”,将来可借鉴其表述。

在我国《个人信息保护法》的制定过程中,就是否应规定数据可携带权原本就有相当大的争议,所以第45条也做了和缓化处理:^[59]个人信息处理者在收到个人信息主体的信息转移或传输请求时,只有“符合国家网信部门规定条件的”,才应该提供转移的途径。即使是赞成可携带权的学者,主要论据也是此举有助于预防和制止平台经济领域的垄断行为,促进市场公平竞争,激励技术创新,维护消费者利益和社会公益。^[60]然而,劳动关系的语境下并不需要追求打破用户锁定效益、防止企业数据垄断的目的,反而可能出现反对引入可携带权的学者提到的风险,比如劳动者个人信息的转移不但会增加个人隐私泄露的风险、给企业带来不小的经济负担,^[61]还容易影响到同事等第三人的个人信息以及用人单位商业秘密的保护。此外,对于劳动者最可能主张可携带权的场景,即解除或终止劳动合同后的档案转移,《劳动合同法》第50条已经规定了用人单位的义务。所以,目前不宜在劳动基准法中赋予劳动者可携带权。

面对劳动关系中应用自动化决策带来的歧视、压榨、误判等危害,一禁了之显然不是正确的选择。且不谈效率低下的问题,人类决策也不能避免前述风险,所以法律规制应重点关注如何减少自动化决策方式带来的额外不利影响。聚焦到劳动基准的问题上,按照《个人信息保护法》第24条要求用人单位保证决策过程的透明度和结果的公平、公正,并赋予劳动者针对自动化决策要求用人单位予以说明的权利和拒绝权,有益却作用有限。算法的可解释性受到了诸多质疑,^[62]单个劳动者在职期间行使该项权利的机率也不大。更有效的或许是在引入自动

[59] 参见龙卫球主编,见前注[56],第206页。

[60] 参见程啸,见前注[45],第343—345页;汪庆华:“数据可携带权的权利结构、法律效果与中国化”,《中国法律评论》2021年第3期,第189—201页。

[61] 参见卓力雄:“数据携带权:基本概念,问题与中国应对”,《行政法学研究》2019年第6期,第129—144页。

[62] 参见丁晓东:“论算法的法律规制”,《中国社会科学》2020年第12期,第142—145页。

化决策机制时,根据《劳动合同法》第4条认定此举属于直接涉及劳动者切身利益的重大事项,要求用人单位就其对劳动者的权益影响向职工代表大会或者全体员工做出解释,并就相关方案进行平等协商。拒绝权行使的前提是决定由算法单独做出、没有任何的人为影响,用人单位却很容易宣称算法只是起到辅助作用、自己保留了最后决策权,劳动者很难验证和证明是否的确如此。行使拒绝权的法律效果如何也有待厘清,比如用人单位在招聘时使用简历自动筛选系统的,被过滤掉的候选人主张拒绝权的后果是什么?劳动基准法立法时还应补充两点:一是避免劳动者“被透视”,坚持数据最小化原则和目的限制原则,不允许用人单位对劳动者进行全面监控、观察记录劳动者的一言一行,即一开始就不提供相应的个人信息基础,对于用人单位出于不同目的收集的各种类型的个人信息原则上也应该分开保存和处理,从而达到限制对劳动者进行数字画像^[63]的目的;二是强调算法取中,不得任由用人单位追求“最优解”。市场监督管理总局、网信办、人力资源社会保障部等七部门于2021年7月26日出台的《关于落实网络餐饮平台责任切实维护外卖送餐员权益的指导意见》要求各平台不得将“最严算法”作为考核要求,而是通过“算法取中”等方式合理确定订单数量、在线率等考核要素,适当放宽配送时限,将来应坚持并推广这一立场。

(六)主管机构、救济方式与法律责任的协调

虽然立法时有过争论,但是我国目前并未将个人信息保护监管职责统一到一个部门,而是在《个人信息保护法》第60条规定由国家网信部门统筹协调、有关部门在各自领域内各司其职。^[64]劳动基准法出台后,增强劳动监察的力量是大势所趋,将来中央与地方各级人力资源社会保障部门应该在内部设置专门的个人信息保护机构、配备个人信息保护方面的专门人员,负责履行劳动用工领域的个人信息保护职责。具体分工上可以由人力资源和社会保障部门专设的个人信息保护机构进行日常的宣传教育、指导监督工作,劳动保障监察机构则接受和处理劳动者与个人信息保护有关的投诉、举报。对于劳动用工领域较为简单、涉及人数较少、违法程度较轻的违法个人信息处理活动,由劳动保障监察机构进行初步的调查和处理;较为复杂的、涉及人数较多、违法程度较重的违法个人信息处理活动,则交由人力资源和社会保障部门专设的个人信息保护机构处理;专业问题极为复杂、涉及人数众多、违法程度严重的,应由人力资源和社会保障部门与同级网信部门一起调查处理。

在救济方式上也不能太过依赖行政力量的介入,而应该在劳动者愿意主动维权时给予制度设计上的支持。《劳动合同法》第38条赋予了劳动者在用人单位有严重违法或违约行为下的“被迫辞职权”,按照其第1项的规定,劳动者以用人单位“未按照劳动合同约定提供劳动保护或者劳动条件”为由解除劳动合同并主张经济补偿金的,法院应当支持。按照传统观念,劳

[63] 有德国学者提出,为避免劳动者沦为“被评价的客体”,应该禁止对其进行人格画像, vgl. Däubler, a.a.O., S. 116.

[64] 参见程啸,见前注[45],第457页。

动保护更多针对生产安全和身体健康,劳动条件则多指工作所需的场所、设施、用品等,^[65]将来应该更新观念,认定个人信息保护也属于劳动保护的范畴,或者直接将“用人单位严重侵害劳动者个人信息权益的”情形列入其中。

涉及用人单位违法处理劳动者个人信息的法律责任,《个人信息保护法》第七章的规定已经相当完备,需要解决的更多是协调性问题,尤其是行政处罚方面。现行法对于用人单位违反劳动基准相关规定的行政处罚力并较小,以违反劳动安全保护的罚款为例,《安全生产法》第99条第5项规定,生产经营单位未为从业人员提供符合国家标准或者行业标准的劳动防护用品的,责令限期改正,处五万元以下的罚款,逾期未改正的,处五万元以上二十万元以下的罚款;而根据《劳动保障监察条例》第23条第7项,用人单位安排未成年工从事矿山井下、有毒有害、国家规定的第四级体力劳动强度的劳动或者其他禁忌从事的劳动的,按照受侵害的劳动者每人1000元以上5000元以下的标准计算处以罚款。相较之下,用人单位违法处理劳动者个人信息或者处理劳动者个人信息未履行保护义务的,按照《个人信息保护法》第66条应责令限期改正,拒不改正的可处一百万元以下罚款,情节严重的可处五千万元以下或者上一年度营业额百分之五以下罚款。就用人单位违法行为的过错程度而言,前述危害劳动者生命健康安全的行为不会低于侵犯劳动者个人信息权益的行为,处罚幅度却明显不一致,将来是调高前者还是降低后者有待思量。

四、结 语

当种种充满赛博朋克意味的场景出现在劳动世界里,可能有人会问,科技发展真的会让人类生活更美好吗?像“卢德分子”那样反对技术进步显然并非正途,我们需要努力的是尽量用法律去纠偏。随着工作设备、工作过程和工作对象的日益数字化,用人单位处理劳动者个人信息更为彻底和全面,劳动者被监视、分析、预测、控制的风险加大,可能威胁到劳动者的人格尊严、自由发展与其他人身和财产权益。作为保护劳动者利益的强行性法律规范,劳动基准法应该与时俱进地加强劳动者的“数字人权”保护,^[66]增加个人信息保护的内容。《个人信息保护法》已经就个人信息保护和利用的冲突解决设定了一般规则,所以劳动基准法的任务在于基于劳动关系的特殊之处进行相应调整。将来应该限制知情同意规则的适用,满足用人单位人力资源管理的正当需求,修改删除权、可携带权和自动化决策条款,协调主管机构、救济方式和法律责任。针对入职面试与体检、背景调查与职场黑名单、工作场所的视频监控、电话监听和局

[65] 参见杨景宇、信春鹰主编:《中华人民共和国劳动合同法解读》,中国法制出版社2007年版,第119页。

[66] 参见吴文芳、刘洁:“新技术变革时代人的变迁与社会法回应”,《学术月刊》2021年第8期,第117页。

域网监控、行踪轨迹与生物识别信息的处理等典型场景，^{〔67〕}还需用劳动基准法的配套文件进一步细化规则。

Abstract: The protection of personal information of workers has its particularities. Specifically, they manifest as the failure of the rule of informed consent in the context of the subordination of weak labor facing strong business, the risk of workers being subject to surveillance and manipulation in the digitalized workplace, and the need to process personal information in the cooperative relationship of organized production. Therefore, the general rules of the Personal Information Protection Law (PIPL) cannot be completely applied in this respect. The Labor Standards Law has been put on the legislative agenda, and it includes, among other things, special provisions concerning the protection of workers' personal information. This is a response to the new challenges of the protection of human rights in the digital era and has great significance to the realization of other labor standards. In labor relations, the protection of personal information cannot only rely on private law, but also needs the intervention of public power at the same time. This is exactly in line with the dual protection mechanism of the law on labor standards, too. Therefore, as a special law for the protection of personal information in labor relations, the law on labor standards should in its relevant provisions consider how to adjust the general rules of the PIPL, including restricting the application of the rule of informed consent, meeting the legitimate needs of human resources management, modifying the provisions regarding the right to delete, the right to data portability, and automated decision-making, and coordinating competent authorities, remedies and legal responsibilities. As the term "necessary" used in the PIPL is a "context-dependent" concept, appropriate documents should be adopted in the future to regulate typical application scenes such as video surveillance in the workplace.

Key Words: Labor Standards Law; Personal Information Protection; Digitalization; Human Resources Management

(责任编辑: 阎天)

〔67〕 就其中部分典型场景已有学者进行研究,参见谢增毅:“职场个人信息处理的规制重点——基于劳动关系的不同阶段”,《法学》2021年第10期,第167—180页。