



中國人民大學

學報

工作论文系列

Working Paper Series

劳动者个人信息法律保护的挑战与应对

丁晓东

JRUCWP2022006

2022. 1. 18

* 本刊编辑部将那些已通过审稿程序而处于“拟录用”状态的稿件制作成线上展示的工作论文，旨在及时传播学术研究成果而促进学术进步。编辑部还将继续与作者共同努力，修改完善论文，并在其达到刊发标准之后择期正式刊发。当然，若工作论文被发现存在严重的质量问题，则仍有可能被退稿。

劳动者个人信息法律保护的挑战与应对

丁晓东

[摘要] 劳动者个人信息保护面临隐私权与个人信息保护二元框架、个人信息处理合法性基础、具体权利义务适用等方面的挑战。究其原因，个人信息保护法与劳动法所调整的都是具有一定支配性的不平等关系，而且其关系都兼具合作性与对抗性。二者的问题叠加使得劳动者个人信息保护不能简单套用个人信息保护的一般框架。应当坚持信义义务与实用主义原则，在兼顾用人单位人力资源管理需求的同时，要求用人单位承担企业的个人信息治理责任，为劳动者个体与集体提供安全与可信赖的个人信息处理。在制度上，应根据不同场景适用个人信息保护的相关制度，实现个人信息保护与劳动者保护的双重目标。

[关键词] 劳动保护；不平等；个人信息；信义义务；实用主义

劳动者个人信息保护是一个历史性难题。在西方的劳资关系发展史上，用人单位常常借用各种手段，对工作场所与劳动者进行监控，以达到保护劳动安全、促进工作效率、阻挠劳工运动的目的。早在19世纪中期，为了帮助用人单位执行企业纪律、监督工会，一位名叫阿伦·平克顿（The Pinkertons）的人成立了侦探局，为企业提供监视用人单位的种种服务。^① 这种服务最终导致美国国会通过了《反平克顿法案》，禁止联邦政府雇佣平克顿或任何类似组织。^②

到了20世纪，随着福特主义与泰勒制的兴起，工厂开始推广标准化、自动化的生产模式，企业的管理也开始专业化与标准化地培训工人，通过研究工人的工作流程与生产过程，为工人制定可以量化的工作强度与考核标准，以此调动工人的积极性，避免企业存在生产混乱、磨洋工等现象。^③ 与20世纪前企业对个人信息的侦探性收集与利用相比，福特主义与泰勒制下用人单位对雇员信息的监控形成了一套体系性的制度，用人单位对雇员的系统性监控进一步增强。“亨利·福特拿着秒表在工厂里徘徊的形象”，成了现代工业时代雇员监控的经典形象。

进入20世纪六七十年代以来，伴随着西方信息技术的发展，用人单位对个人信息的收集进入一个新阶段，开始从工业化的收集迈向信息化时代的收集。例如刷卡代替了原先的签到，工作场所的24小时视频监控代替了原先的用人单位巡视。^④ 伴随着现代科技层出不穷地新应用，个人信息

作者：丁晓东，中国人民大学法学院副教授，dingruc@163.com。

* 本文系国家社会科学基金重大项目“我国社会法的概念、原则、理论与实践”（18ZDA140）的阶段性成果。

① Frank Morn. *The Eye That Never Sleeps: A History of the Pinkerton National Detective Agency*. Indiana University Press, 1982, p. 18.

② Pub. L. No. 89-554, 80 Stat. 416. (1966).

③ Taylor Frederick Winslow. *The Principles of Scientific Management*. The Floating Press, 2012.

④ Ball K. "Workplace Surveillance: An Overview". *Labor History*, 2010, 51 (1): 87-106.

的收集呈现出急遽加速的趋势。有的用人单位关注个人在社交网络的各种信息、发言甚至是网站浏览记录，有的用人单位利用为员工提供的各类佩戴设备，全天候地获取雇员的位置、健康等信息。^①

在政策与法律应对层面，各国对雇员的个人信息保护一直保持高度关注。国际劳工局于1997年发布了《保护劳动者个人数据行为守则》，提出了收集与处理劳动者数据的十三项准则。^② 20世纪80年代，美国技术评估办公室（United States Office of Technology Assessment）出版了《电子监控：新技术、新紧张局势》的报告。^③ 欧盟2018年生效的《一般数据保护条例》第88条对雇员信息保护做了专门规定，第29条工作小组随后针对工作场所的数据处理出台指导意见。^④ 整体而言，当前美国对劳动者个人信息的保护仍然处于传统隐私权保护与若干单行法律保护的阶段，而欧盟则由于其1995年制定的《数据保护指令》与2018年生效的《一般数据保护条例》，对劳动者个人数据提供了更为严格的保护。

2021年8月20日，我国《中华人民共和国个人信息保护法》（下文简称《个人信息保护法》）通过，我国的劳动者个人信息保护也迎来一个全新的阶段。我国的《个人信息保护法》采取了类似《一般数据保护条例》的综合立法模式，对不同行业与场景下的个人信息保护做出了统一规定。在此之前，其他大量的法律法规也对个人信息进行不同角度的保护，例如《网络安全法》《民法典》人格权编，都专门制定了个人信息条款。

本文所要解决的问题是，在个人信息保护综合立法的背景下，劳动者个人信息保护面临哪些挑战？^⑤ 这些挑战的背后原因与形成原理是什么？如何通过制度设计回应此类挑战？本文认为，劳动者个人信息保护面临隐私权与个人信息保护二元框架、劳动者个人信息处理合法性基础、个人信息权利与信息处理者义务适用等多方面的挑战。其原因在于，劳动者保护与个人信息保护都具有不平等性、持续支配性、兼具合作性与对抗性等特征，而且二者的问题叠加使得这些特征更为明显。为了解决这些问题，本文提出以信义义务和实用主义原则为指导，要求用人单位承担企业的个人信息治理责任，协调劳动者个体与集体需求。在制度设计上，本文以求职、工作场所、工作场所之外等场景为例，提出不同场景下的个人信息保护制度设计。

一、劳动者个人信息保护的挑战

如上所述，我国个人信息保护采取综合立法模式。这种模式的优点是可以适用于所有主体，包括劳动者、消费者与其他信息主体或数据主体。但就劳动者个人信息保护而言，此类综合立法模式也存在若干挑战。

（一）隐私与个人信息二元框架的挑战

首先，隐私与个人信息的二元保护框架能否有效保护劳动者，存在争议。按目前的隐私权与个

^① Brassart Olsen C. "To track or not to track? Employees' data privacy in the age of corporate wellness, mobile health, and GDPR". *International Data Privacy Law*, 2020, 10 (3): 236 - 252.

^② "The ILO's code of practice on the protection of worker's personal data". *International Labour Review*, 1996, 135 (5): 577.

^③ "The Electronic Supervisor: New Technology, New Tensions". Washington, D. C.: Congress of the United States, Office of Technology Assessment, 1987.

^④ Article 29 Working Party, Opinion 2/2017 on data processing at work (17/EN WP 249) (June 8, 2017), p. 7, <https://ec.europa.eu/newsroom/article29/items/610169>.

^⑤ 从隐私权角度进行的分析已经积累了不少成果，相关综述参见喻术红、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（5）。

人信息保护法,二者首先存在不同的适用范围。简单来说,隐私权可以适用于所有的关系,只要存在侵犯隐私的情形,法律都可以将二者拟制为侵权关系进行调整。相反,对于个人信息保护,其适用前提则是存在个人信息处理关系。例如我国《个人信息保护法》第3条规定:“在中华人民共和国境内处理自然人个人信息的活动,适用本法。”欧盟《一般数据保护条例》将适用范围界定为“全自动个人数据处理、半自动个人数据处理,以及形成或旨在形成存档系统的非自动个人数据处理”,同时在“重述”中明确,《条例》不适用“与专业或商业活动无关的个人或者家庭事务”的个人数据处理,以及在自动化或半自动化情形下“未按照特定标准构建的档案或档案集及其封面”的情形。^①

按照这个标准,当用人单位采取自动化或半自动化手段,或者系统性地对个人信息进行建档而收集个人信息,则其活动属于《个人信息保护法》或《一般数据保护条例》等法律的适用范围^②;但如果用人单位没有进行此类活动,仅仅在日常工作交往中获取个人信息,则此类行为不在一般个人信息保护法的适用范围,只能适用于传统隐私权保护。我国和欧盟等国家和地区的法律都将自然人因为“个人或者家庭事务”而处理个人信息的情形排除在个人信息保护之外。^③

隐私权保护与个人信息保护的这种二元划分有其合理之处,因为隐私权保护主要针对信息能力平等或拟制为平等的主体。无论是大陆法系人格权体系下的隐私权保护^④,还是美国的隐私侵权^⑤,所保护的都是个体在社会中的“社交规则”。^⑥但个人信息保护则相反,个人信息保护针对的是信息能力不平等或拟制为不平等的主体^⑦,其保护的是一种通过信息技术或手工大规模建档的信息处理关系。如果将平等民事主体之间的信息关系也纳入个人信息保护范畴,将会导致普遍违法。法律不可能将所有未经他人同意打听他人信息均认定为违法,个人也不可能向信息获取者行使查询复制权、更正权、删除权等权利主张。

但在劳动用工的场景下,隐私权与个人信息保护的二元法律框架面临不少挑战,可能都无法有效保护劳动者。由于雇佣关系本身的从属性与支配性,用人单位或其管理者常常能够比较容易获得劳动者个人信息;特别是随着社交媒介的兴起,用人单位及其管理者更是可以毫无障碍地大量获取个人信息。^⑧但是悖论的是,劳动者可能在很多情形下既无法通过隐私侵权寻求保护,又无法通过个人信息保护法寻求保护。一方面,用人单位获取的很多信息可能属于公共信息,无论是日常生活和工作中获取的信息,还是社交媒介的信息,可能都无法满足隐私侵权的救济要件。另一方面,用人单位所获取的信息可能是偶然性的,并没有利用自动化或半自动化手段进行处理,也没有对个人

① 《一般数据保护条例》第2条第1款、重述第18条、重述第15条。

② 王倩、顾雪莹,《GDPR下涉欧企业的员工个人数据合规管理》,载《德国研究》,2021(2)。

③ 《一般数据保护条例》第2条(c);《中华人民共和国个人信息保护法》第72条。

④ Paul M. Schwartz and Karl-Nikolaus Peifer. "Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?". *California Law Review*, 2010, 98 (6): 1925.

⑤ Samuel D. Warren and Louis D. Brandeis. "The Right to Privacy". *Harvard Law Review*, 1890, 4 (5): 193-220.

⑥ Robert C. Post. "The Social Foundations of Privacy: Community and the Self in the Common Law Tort". *California Law Review*, 1989, 77 (5): 957.

⑦ 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》,载《中外法学》,2020(2)。

⑧ Sanders SD. "Privacy Is Dead: The Birth of Social Media Background Checks". *Southern University Law Review*, 2012, 39 (2): 243-264; Patricia Sánchez Abril, Avner Levin and Alissa Del Riego. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee". *American Business Law Journal*, 2012, 49 (1): 63-124; Pham HH. "Bloggers and the Workplace: The Search for a Legal Solution to the Conflict between Employee Blogging and Employers". *Loyola of Los Angeles Entertainment Law Review*, 2005, 26 (2): 207-236; 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》,《华中科技大学学报》(社会科学版),2019(3)。

信息建立档案系统。这样，用人单位或其管理者与个人之间可能就没有成立个人信息处理关系，不适用个人信息保护法的规定。但毫无疑问，由于劳动关系本身具备支配性与从属性，即用人单位收集的是公开信息，且此类信息没有进行系统化存档，过多的劳动者个人信息收集也可能对劳动者产生威胁。

其次，个人信息保护法适用的另一个挑战是，何种情形下小微企业构成个人信息保护法适用的豁免？对于此类豁免，我国的《个人信息保护法》进行了明确规定，第62条规定国家网信部门统筹协调有关部门制定“针对小型个人信息处理者”的规则。在《个人信息保护法》的立法过程与专家研讨中，立法起草者与专家学者对小型信息处理者的豁免或责任减轻也有一定共识。欧美的相关立法也对此有较为明确的规定。

在消费者个人信息保护的场景下，对便利店、小作坊进行个人信息保护法豁免，这具有很强的正当性，因为这些小微企业更类似民事主体，对个人信息不具备超大规模的收集与处理能力，也不具备设置专业人员的能力。但在劳动用工关系中，这种豁免也可能带来一定的悖论。因为相比大型企业，小微企业的用人单位与员工恰巧更为熟悉，而且更容易随意调取各类技术手段收集而来的员工信息，一旦企业收集劳动者大量个人信息，并且结合日常劳动管理场景利用此类信息，小微企业的用人单位就可能对员工造成更大的威胁。^①相反，大型企业中企业与员工的关系更为科层化，其对劳动者个人信息的收集与监控也相对规范。如果对大型企业无条件施加个人信息保护的一般责任，对小微企业无条件豁免或克减个人信息保护的一般责任，这反而不利于对劳动者进行保护。

（二）合法性基础的挑战

劳动者个人信息保护的第二个挑战在于个人信息处理的合法性基础。目前，我国《个人信息保护法》第13条规定了处理个人信息的七项情形，包括个人同意、合同必需“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”、履行法定职责或者法定义务、应对突发公共卫生事件、在合理的范围内处理已公开的个人信息、新闻报道、舆论监督等。其中“人力资源管理所必需”的表述为立法过程的最后一刻加入。相较欧盟《一般数据保护条例》的规定，我国并未单独将“正当利益”列为处理个人信息的合法性基础，而是在“合同必需”一项中补充人力资源管理这一情形，在一定程度上是为了实现“控制者或第三方所追求的正当利益（legitimate interest）”的限缩。^②在《个人信息保护法》起草过程中，企业正当利益特别是劳动用工场景下企业正当利益一再被提起，最终立法者纳入了人力资源的限定条件，但并没有效仿欧盟使用“正当利益”的宽泛表述。

在用工场景下，企业的正当利益或“人力资源管理所必需”主要包括监控和保护公司财产，包括保护公司的有形财产和知识产权，设置企业合理的激励制度，为劳动者提供合理的报酬，提高劳动者的生产效率。在劳动关系中，用人单位与劳动者之间并不总是能够通过计件或标准化任务完成的方式进行考核，如果能进行此类考核，用工主体与劳务提供者之间就会形成承揽关系或劳务关系等民事关系，而非具有从属性的劳动关系。正是因为很多工作是非标准化的，用人单位与劳动者之间形成以“控制与从属”为基本特征的劳动关系，用人单位对劳动者具有一定的管理权，企业正当利益或“人力资源管理所必需”也成为个人信息处理的合法性基础^③，但这也对劳动者个人信息保护提出了挑战。正如上文所述，在劳动用工的场景下，劳动者个人信息所面临的风险要远大于消费

^① 《员工工作手机通话数据是否属于个人隐私？判决来了！》，参见 <https://mp.weixin.qq.com/s/jZFxnDzP3WhOM8elo2m4Sw>。

^② 《一般数据保护条例》第6条。

^③ 《一般数据保护条例》重述第48条明确规定：企业“出于内部管理目的在企业组内传输包括处理客户或员工的个人数据，这属于企业正当利益”。

者等场景，因为用人单位对于劳动者更为熟悉，更具有支配力。在这种背景下，企业的正当利益与劳动者个人信息保护需求之间的关系将更为紧张。^①

劳动者个人信息处理合法性基础的另一挑战是告知同意原则。虽然包括我国在内的所有国家都将同意作为个人信息处理的一般合法性基础，但在劳动用工的场景下，这一基础是否适用仍然存疑。这不仅关涉到告知同意的一般困境，例如个人没有时间阅读、不容易理解信息处理者的告知，^② 在劳动用工的场景下，其中更严重的问题是劳动者是否有可能做出真正有意义的选择。出于工作需要，劳动者一般都会同意用人单位的信息收集。特别是当劳动者获取工作之后，出于对工作稳定性的需求，劳动者更难拒绝用人单位所提出的各类信息收集要求。也因此，很多国家和地区的法律指引都质疑了告知同意原则的有效性。例如欧盟第 29 工作组指出：“对于大多数员工数据处理案例，处理的法律基础不能也不应该是员工的同意。”^③

（三）权利义务适用的挑战

劳动者个人信息保护的第三个挑战在于个人信息保护中的权利义务适用。各国的个人信息保护制度均继承了“公平信息实践”的框架^④：一方面，赋予个体以知情选择权、查询复制权、更正权、删除权、脱离自动化处理权、携带权等权利；另一方面，则对信息处理者施加各种义务，在满足个体信息权利的同时承担目的限制、信息最小化、限期储存、信息安全、信息质量等义务。^⑤ 但是，这种权利与义务的制度设计一旦落到各种劳动用工的各种场景，就会发现有的权利与义务未必适用。

就劳动者的信息权利而言，劳动者在视频监控等很多场所下就未必有权行使其查询复制权、携带权等权利。尽管查询复制权或访问权常常被认为是个人信息权利中的一种基本权利^⑥，但在很多场景下，用人单位或用人单位所收集的个人信息往往多人混同，当个人提起信息查询复制权的主张，要求复制此类视频，甚至提出要求大规模复制此类视频，则此时就很可能侵犯他人的信息权利。尽管工作场所具有一定的公共性，但如果每位员工都可以调取和复制此类视频，则等于每位劳动者都将暴露于他人的 24 小时监视之下，劳动者的隐私与个人信息将遭受重大威胁。同样，劳动者对于工作场所监控的信息删除权也面临争议，因为此类监控可能需要保存一段时间，以防在一些问题出现时对其进行调用取证。除非此类视频涉及劳动者的某些私密信息或活动，否则个体所提出的删除权可能很难主张。

就用人单位的信息责任而言，有的责任可能适用于所有场景，但其他有的责任则可能在有的场景下适用，在其他场景下不适用。例如信息安全的责任对于所有场景可能都适用，但限期储存的责任可能会与用人单位的安全保障义务具有一定冲突，用人单位具有保存数据一段时间的正当需求。而对于信息质量而言，在有的场景下，高清画质以及具有高识别度的个人信息收集可能有利于精准

^① Fisk CL. "Privacy, Power, and Humiliation at Work: Re-Examining Appearance Regulation as an Invasion of Privacy". *Louisiana Law Review*, 2006, 66 (4): 1111.

^② Solove DJ. "Introduction: Privacy Self-Management and the Consent Dilemma". *Harvard Law Review*, 2013, 126 (7): 1880 - 1903.

^③ Article 29 Working Party, Opinion 2/2017 on data processing at work (17/EN WP 249) (June 8, 2017), pp. 6 - 7, <https://ec.europa.eu/newsroom/article29/items/610169>.

^④ Rotenberg M. "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)". *Stanford Technology Law Review*, 2001, 2001: 1 - 34.

^⑤ Schwartz PM. "Privacy and Democracy in Cyberspace". *Vanderbilt Law Review*, 1999, 52 (6): 1607 - 1702.

^⑥ 例如我国《民法典》与《个人信息保护法》都规定了这种权利，欧盟则不仅在《一般数据保护条例》中规定了这种权利，而且在《欧盟基本权利宪章》中也规定了这一权利。参见《民法典》第 1037 条；《个人信息保护法》第 45 条；《一般数据保护条例》第 15 条；《欧盟基本权利宪章》第 8 条。

识别劳动者，从而为劳动者提供更好的服务与实施更方便高效的人力资源管理；但在其他场景下，用人单位采取模糊化的视频监控，可能既可以实现其正当利益，又可能防止对劳动者对隐私与个人信息造成过多侵扰。

二、劳动者个人信息保护的原理反思

劳动者个人信息保护为何面临挑战？从原理层面分析，可以发现劳动者个人信息保护面临个人信息保护的一般性问题与劳动用工场景下的特殊性问题。由于个人信息保护所涉及的关系具有不平等性、关系持续性、兼具合作对抗性，导致个人信息保护具有权利相对不确定性、场景依附性、制度弹性等特征。在劳动者场景下，上述特征与原因进一步放大。

（一）个人信息保护的一般性

首先，个人信息权利具有一定的不确定性。从隐私保护到个人信息保护，这虽然已经成为我国和很多国家的共识，但除了隐私权的那部分法益，个人信息保护到底保护什么？这仍然是一个有争议的问题。从是否需要保护来看，强调个人信息流通共享的观点认为，只要个人信息收集与处理不涉及隐私性权益，就不应该从法律层面立法保护个人信息^①；而相反的观点则认为，收集与处理个人信息本身就构成了一种威胁。^②从权利的性质角度看，个人信息权利可能与人格权相关，保护个人信息可能是为了保护个人的人格不被侵害^③，但个人信息权利也可能和个人的财产性权益与风险防御等权益相关。^④从比较法来看，欧盟将个人信息被保护的权利上升为一种基本权利，对个人信息更多采取公法规制^⑤，而美国则主要将其视为一种消费者权利，对其预留了更多私法自治的空间。^⑥以上种种争论都反映了个人信息保护不像隐私保护那样达成更高共识。

其次，个人信息保护具有场景依附性。个人信息保护与财产权等有形物的保护并不相同，如果说有形物的保护是保护物体本身，那么个人信息保护保护的是不同场景下个人信息被收集、储存、加工、利用、流转这一系列行为操作，而非个人信息本身。这其中的原因在于，土地、财产等有形物不会因为场景的变化而发生太多的变化，但个人信息则可能因为其收集者、处理者、处理者与个人之间的关系、行业规范、信息性质的不同而不同。^⑦这也正是为何欧盟等地区和国家在进行综合统一立法后，都通过监管机构进一步发布各类场景化的指南。

最后，个人信息保护法所采取的制度具有较大弹性。我国和欧盟等国家均采用综合立法的个人信息保护体例，这种体例的优势是法条较为清晰明确、适用范围较广。但从制度弹性来看，其制度弹性要超过很多常见的法律，甚至超过美国所采取的消费者隐私保护法的立法路径。^⑧因为这种制

^① Ben-Shahar O and Strahilevitz LJ. "Contracting over privacy: Introduction". *Journal of Legal Studies*, 2016, 45 (2): 1-11.

^② Solove DJ. "Privacy and Power: Computer Databases and Metaphors for Information Privacy". *Stanford Law Review*, 2001, 53 (6): 1393-1462.

^③ Bloustein EJ. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser". *New York University Law Review*, 1964, 39 (6): 962-1007.

^④ Victor JM. "The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy". *Yale Law Journal*, 2013, 123 (2): 513-529.

^⑤ Schwartz PM. "Global Data Privacy: The EU Way". *New York University Law Review*, 2019, 94 (4): 771-818.

^⑥ FTC Staff. "Protecting Consumer Privacy in an Era of Rapid Change - A Proposed Framework for Businesses and Policy-makers". *The Journal of Privacy and Confidentiality*, 2011, 3 (1).

^⑦ Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009, p. 141.

^⑧ Chander A, Kaminski ME and McGeeveran W. "Catalyzing Privacy Law". *Minnesota Law Review*, 2021, 105 (4): 1733-1802.

度其实采取了一种公私法高度融合^①、具有广义社会法特征的合作治理路径，其中公法规制与私法自治的界限并不特别明确。^② 再加上上述个人信息权利的相对不确定性、个人信息保护的场景依附性，就会让个人信息保护法中有的权利与责任因场景的不同而变换。相对而言，美国的立法路径则对特殊领域进行更为刚性的规制立法，对其他领域给予更多私法自治的空间，这使得美国个人信息保护中公法规制与私法自治的界限更为清晰。

从成因来看，个人信息保护之所以具有这些特征，是因为个人信息保护所涉及的是具有不平等性、关系持续性与兼具合作对抗的关系。信息处理者与个人之间由于信息能力上的持续性不平等，二者构成了支配型关系。而他们之间又并非简单地对抗关系，在很多情形下，信息处理者既可能利用其信息优势支配个人，但也很可能利用信息为个人提供更好服务和安全保障。

（二）劳动者个人信息保护的特殊性

劳动者个人信息保护具有个人信息保护的一般性特征，但也具有特殊性。其特殊性在于，即使不存在个人信息处理关系，劳动关系中用人单位与劳动者之间也具有不平等性、关系持续性与兼具合作对抗性。一方面，在劳动关系确立后，用人单位可以对劳动者进行指挥与管理，二者具有持续不平等的人身从属性或支配型关系^③；另一方面，用人单位既可能侵犯劳动者权益，但也可能和劳动者形成互惠合作的关系。因此，上述个人信息保护法的一般性特征，在劳动者个人信息保护中会被进一步放大。

首先，劳动者个人信息权利更不确定，个人信息保护与隐私保护的界分更不明确。就一般制度而言，个人信息保护与隐私保护区分的关键在于是否存在处理行为，如果不存在处理行为，则双方构成罗伯特·波斯特所谓的侵权隐私保护或“尊严隐私”；如果存在处理行为，则双方构成个人信息保护或“数据隐私”。^④ 但是，由于用人单位与劳动者本身的持续性不平等和合作对抗共存关系，即使非处理的个人信息收集，也可能产生个人信息保护所要处理的持续性不平等问题，需要在对劳动者的隐私权进行特殊保护。^⑤ 此外，虽然个人信息保护法对小微企业进行豁免，但劳动用工场景下的小微企业完全可能对劳动者造成同样的信息威胁，甚至可能造成比大型企业更大的信息威胁。

其次，劳动者个人信息保护的场景性更突出。这不仅是因为劳动用工本身就构成一种行业场景，区别于教育、金融、消费、医疗等场景^⑥，而且还因为用人单位与劳动者之间的复杂关系，二者之间常常存在更多场景混同。例如二者之间常常存在工作场景与生活场景的混同，用人单位对劳动者的生活关心，本来属于日常交往中的信息规则，但在特定场景下，又可能转化为工作上的支配。用人单位了解到劳动者可能准备生二胎，就可能导致其对劳动者的另类对待。^⑦ 在我国职场氛围中，这种工作关系与生活关系混同的情形更为普遍，也因此使得劳动者个人信息保护更具场景化。

① 作为公私法融合的社会法，参见吴文芳：《新技术变革时代“人”的变迁与社会法回应》，载《学术月刊》，2021（8）。

② Kaminski ME. “Binary Governance: Lessons from the GDPR’s Approach to Algorithmic Accountability”. *Southern California Law Review*, 2019, 92 (6): 1529 - 1616.

③ 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（2）。

④ Post RC. “Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere”. *Duke Law Journal*, 2018, 67 (5): 981 - 1072.

⑤ 潘峰：《论劳动者隐私权的法律保护：一个分析框架》，载《河北法学》，2008（7）。

⑥ 在美国的个人信息保护立法中，此类特殊场景常常单独立法，比如《公平信用报告法》《家庭教育权利与隐私法》《健康保险可携带性和责任法》，分别参见 15 U. S. C. § 1681；20 U. S. C. § 1232g；Pub. L. No. 104 - 191.

⑦ 北京互联网法院所做的著名的微信读书案判决，就与此相关。参见北京互联网法院（2019）京 0491 民初 16142 号民事判决书。

最后，劳动者个人信息保护的制度具有更大弹性。除了个人信息保护的制度弹性之外，劳动者保护本身也一直面临着私法自治与公法规制的紧张张力。在相对支持市场的学者看来，劳动关系更多应该以私法自治的方式进行调整^①；而在相对支持劳动规制的学者看来，劳动关系则呈现资强劳弱的特征，需要倾斜保护。^②因此，劳动法律制度本身就是一种公私法混同的法律制度^③，有关“管制”还是“放松”的讨论持续存在。^④例如不同学者对于学历要求、年龄要求是否构成就业歧视，需要法律规制，就有不同看法^⑤；近年来讨论颇多的平台用工规制领域，亦出现有关更多发挥市场自治还是更多赋予劳动保护的争论。^⑥当劳动者保护中的制度争议叠加个人信息保护中的制度争议，就会使得劳动者个人信息保护中的有关制度设计更具复杂性。

三、劳动者个人信息保护的原则重构

面对劳动者个人信息保护的双重挑战，法律应当按照何种原则进行制度设计？这一部分提出，可以引入信息信义义务原则和实用主义原则保护劳动者个人信息，根据不同场景而适用个人信息保护法中的有关制度，避免对用人单位进行全有或全无的规制。

（一）信义义务原则

在个人信息保护的研究与实践中，信义义务的原则就已经被提出，以应对个人信息保护的若干困境。个人信息保护法的研究已经表明，面对个人与平台等企业之间的专业能力差距，个人常常难以通过传统合同法进行真正的个人信息自我管理，也难以通过传统侵权法进行救济。^⑦对此，巴尔金等教授提出了个人信息保护的信义法保护方案，以对传统私法进行转型升级。他指出，信息处理者与个人之间的关系与信义义务所处理的关系具有一定的相似性。在律师与客户、^⑧医生与病人的关系中，^⑨都可能存在专业知识差距与相互依赖的问题。这与平台等信息处理者与个人之间的关系具有类似性，二者既在信息能力方面差距显著，同时个人对于平台又形成一定的依赖。^⑩因此，可以引进信义义务原则，要求平台对个人信息保护承担更高的责任。

信义义务主要包括谨慎义务与忠诚义务。所谓谨慎义务，指的是受托人必须谨慎行事，尽职尽责，以免损害委托人、受益人或客户的利益。而所谓忠诚义务，指的是受托人必须牢记委托人或客

① 董保华：《〈劳动合同法〉的十大失衡问题》，载《探索与争鸣》，2016（4）。

② 常凯：《论劳动合同法的立法依据和法律定位》，载《法学论坛》，2008（2）。

③ 沈建峰：《劳动法作为特别私法——〈民法典〉制定背景下的劳动法定位》，载《中外法学》，2017（6）。

④ 阎天：《供给侧结构性改革的劳动法内涵》，载《法学》，2017（2）；王玉：《网络劳务是对劳动法的挑战吗》，载《中国法律评论》，2018（6）。

⑤ 王月明：《消除年龄歧视是劳动权平等保护的首要内容》，载《法学》，2010（3）；丁晓东：《重新理解年龄区分：以法律手段应对年龄歧视的误区》，载《法学家》，2016（4）。

⑥ 董保华：《劳动关系治理的变革之道——基于“增量”与“存量”的二重视角》，载《探索与争鸣》，2019（1）；王全兴、王茜：《我国“网约工”的劳动关系认定及权益保护》，载《法学》，2018（4）。

⑦ Lorrie Faith Cranor. “Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice”. *J. on Telecomm and High Tech. L.*, 2012, 10: 273 - 308; Calo R. “The Boundaries of Privacy Harm”. *Indiana Law Journal*, 2011, 86 (3): 1131 - 1162.

⑧ ED Spurgeon and MJ Ciccarello. “The Lawyer in Other Fiduciary Roles: Policy and Ethical Considerations”. *Fordham Law Review*, 1994, 62 (5): 1357 - 1410; P. Zwier. “Is the Maryland Director and Officer Liability Statute based on a male-oriented ethical model?” *University of Baltimore Law Review*, 1989, 18 (2): 368.

⑨ MA Rodwin. “Strains in the Fiduciary Metaphor: Divided Physician Loyalties and Obligations in a Changing Health Care System”. *American Journal of Law & Medicine*, 1995, 21 (2 & 3): 241 - 258; M. Oberman. “Mothers and Doctors’ Orders: Unmasking the Doctor’s Fiduciary Role in Maternal-Fetal Conflicts”. *Northwestern University Law Review*, 2000, 94 (2): 451 - 502.

⑩ Balkin JM. “Information Fiduciaries and the First Amendment”. *UC Davis Law Review*, 2016, 49 (4): 1183 - 1234.

户的权益，为客户的利益行事，避免潜在或实际的利益冲突。^① 相比合同义务，合同中的一方只需要按照合同的要求完成任务即可，但在信义法框架中，受托方还需要促进合同规定之外的委托人利益。^②

当然，个人信息保护中的信义义务与一般的信义法仍有较大区别，与狭义的财产信托法（trust law）则更有较大差别。^③ 传统的信义义务是在有偿报酬的前提下形成的，且在很多情形中是一对一关系；财产信托法则更是聚焦于财产关系与责任。但网络平台等信息处理者与个人之间不是一对一的关系，其关系的紧密程度远低于医生和律师等关系中的传统信义法关系，而且网络平台等信息处理者也不直接涉及财产问题。因此，个人信息保护中的信义义务应当被视为一种“基于特定目的的信息信托（special-purpose information fiduciaries）”^④，其目的主要是为了保护用户的隐私权益与信息权益。

在劳动者个人信息保护中，可以寻求一种保护劳动者一般权益与个人信息权益的特定信义义务。一方面，用人单位对于劳动者本身就承担很多义务，在一定程度上具备信义义务的特征。^⑤ 这就是意味着，首先，即使用人单位对劳动者的信息收集不适用个人信息保护法，甚至不适用传统隐私权保护，用人单位也应在相关活动中承担谨慎义务、忠诚义务等劳动法上的信义义务，注重劳动者权益保护。其次，当用人单位的相关信息处理活动涉及个人信息时，用人单位应承担信息信义义务，例如用人单位不能以劳动者同意或授权为由，任意收集与处理个人信息。^⑥ 总之，用人单位应超越一般的合同义务，承担符合劳动者个人信息保护特征的信义义务。

（二）实用主义原则

信义义务原则是一种介于公法与私法之间的原则，它既要求用人单位对劳动者部分履行家长主义的义务，但又给予双方当事人一定自由协商的空间。信义义务的这种特征会使得相关制度的设计具有一定的弹性或不确定性。为了解决这一问题，可以再引入实用主义或功能主义原则，为劳动者个人信息保护的制度设计提供指引。

所谓实用主义原则，指的是对相关法律问题性质与后果的判断不应采取本质主义的立场，而应采取问题导向与工具一目的合理性的制度考虑。^⑦ 具体到劳动者个人信息保护中，这就意味着应当分析不同场景下用人单位与劳动者的信息关系，并根据不同关系适用劳动者保护与个人信息保护的不同制度。从信息关系与制度的对应关系出发，可以为信义原则落地提供指引，为每个不同场景提供不同的劳动者个人信息保护制度。

相反，非实用主义原则的进路则分析某种个人信息处理行为是否适用个人信息保护法，再在个人信息保护法中寻找劳动者相关条款，最后再根据相关条款规定的例外情形、法律后果等情况而进行法律适用。对于经验丰富的法律研究者与实践者来说，遵循这种进路与模式，可能最终也会在很多问题寻找到合理答案，但其效率却未必很高。按照这种进路和模式，可能会遗漏很多重要问题，例如可能在个人信息适用问题上就将很多情形排除在外，从而伤害劳动者利益；或者可能会在

① Tamar Frankel. *Fiduciary Law*. Oxford University Press, 2011.

② Langbein JH. "The Contractarian Basis of the Law of Trusts". *Yale Law Journal*, 1995, 105 (3): 625 - 676.

③ Larry E. Ribstein. "The Revised Uniform Partnership Act: Not Ready for Prime Time". *Bus. Law*, 1993, 49 (45): 53 - 54.

④ Balkin JM. "Information Fiduciaries and the First Amendment". *UC Davis Law Review*, 2016, 49 (4): 1183 - 1234.

⑤ Bodie MT. "Employment as Fiduciary Relationship". *Georgetown Law Journal*, 2017, 105 (4): 819 - 870.

⑥ 谢增毅：《劳动者个人信息保护的法治价值、基本原则及立法路径》，载《比较法研究》，2021（3）。

⑦ Richard A. Posner. *Overcoming Law*. Harvard University Press, 1995, p. 395; Farber DA. "Legal Pragmatism and the Constitution". *Minnesota Law Review*, 1988, 72 (6): 1331; Thomas C. Grey. "Holmes and Legal Pragmatism". *Stanford Law Review*, 1989, 41 (4): 787 - 870.

很多问题上面临非常多的例外，从而对劳动者个人信息保护的体系性与类型化思考构成障碍。

四、劳动者个人信息保护的制度建构

在原理反思与原则建构之后，可以按照上文提到的信义义务原则与实用主义原则进行制度研究。这一部分选取求职与面试、工作信息、生活信息等若干典型场景，结合本文第一部分提到的隐私与个人信息保护二元法律框架、合法性基础、具体权利义务适用等挑战，构建个人信息保护的具体制度。

（一）求职阶段

在求职阶段，劳动者与用人单位之间并未形成劳动关系或支配关系，二者的信息关系与普通信息处理中的关系具有一定相似性，都由信息能力的持续性不平等而造成，不需要系统性地结合劳动关系进行考虑。

就适用范围而言，求职阶段的劳动者个人信息保护可以适用个人信息保护法的一般制度。法律可以适度区分隐私与个人信息保护，对于企业侵害劳动者隐私的行为进行隐私侵权保护，对于企业进行自动化收集或建档的信息收集行为进行个人信息保护，并对小微企业进行一定程度的豁免。因此，当企业相关行为未构成“处理”行为，或者小微企业利用自动化等技术收集个人信息时，此时个人信息保护法未必适用或全部适用。

当然，以上适用也并非绝对。由于求职可能导致劳动关系的形成，求职阶段企业与劳动者的信息关系也可能涉及劳动者权益保护，需要对信息收集与处理进行规制。如果企业对个人信息的收集涉及直接歧视或侵犯公民的人格权，则即使此类信息收集不侵犯劳动者隐私，也不适用个人信息保护法，也应对此类信息收集行为进行一定限制。^①例如在疫情期间，有企业收集求职者是否来自武汉或湖北的信息，此类信息收集行为就应当被禁止。^②

此外，网络招聘服务平台应当适用个人信息保护法的一般制度。近年来，互联网技术与人力资源服务深度融合，网络招聘市场发展迅猛，据人社部披露，网络招聘已经成为劳动者求职和用人单位招聘的主渠道，截至2019年底，全国共建立人力资源市场网站1.5万个，2019年通过网络发布招聘信息4.04亿条、发布求职信息8.23亿条。^③网络招聘服务平台通过互联网等信息网络为劳动者求职和用人单位招聘人员提供求职、招聘服务，涉及大规模个人信息，甚至是敏感个人信息的处理行为，应适用我国《个人信息保护法》。2020年12月，人社部出台《网络招聘服务管理规定》，其中第21条明确规定：“人力资源服务机构从事网络招聘服务时收集、使用其用户个人信息，应当遵守法律、行政法规有关个人信息保护的规定。”我国《个人信息保护法》出台后，《网络招聘服务管理规定》得以与个人信息保护规则衔接，网络招聘服务平台应当遵守个人信息处理规则，承担个人信息处理者的义务，大型招聘平台则更应压实平台责任。^④

^① 田野：《雇员基因信息保护的私法进路》，载《法商研究》，2021（1）；柯振兴：《劳动者的隐私权初探》，载《黑龙江省政法管理干部学院学报》，2014（5）；魏倩：《日本法上的劳动者人格保护——以劳动者健康隐私为中心》，载《科技与法律》，2014（3）。

^② 林嘉：《专家谈42开头身份证被歧视：部分做法触碰法律红线》，参见<https://wap.peopleapp.com/article/5238673/5142068>。

^③ 人社部流动管理司负责人就《网络招聘服务管理规定》答记者问，参见http://www.mohrss.gov.cn/SYrlzyshbzb/dongtaixinwen/buneyiaowen/rsxw/202012/t20201224_406597.html。

^④ 2021年315晚会上，央视曝光了多家大型招聘线上平台个人简历泄露问题，其中智联招聘、猎聘、前程无忧被点名，均为从事网络招聘服务的大型平台，《3·15晚会曝光 | 智联招聘、猎聘平台简历给钱就可随意下载，大量流向黑市！》，参见<https://news.cctv.com/2021/03/15/ARTIVyd2R7kvms6uilsmrD8P210315.shtml?spm=C94212.Ps9fhYPqOdBU.S51378.8>。

就合法性基础而言, 求职阶段的个人信息合理收集应视为符合我国《个人信息保护法》第13条规定的合法性基础条款或欧盟《一般数据保护条例》的正当利益条款。信息处理者对于公开信息或劳动者自愿公开信息的收集不需要以告知—同意为合法性基础, 但需要承担相应义务。这是因为, 在求职阶段, 劳动者与用人单位对于信息共享都有较大需求。离开了信息共享, 人力资源市场就不可能运作, 良好的劳资关系就不可能成型。此外, 由于双方并未建立直接联系, 此时要求企业或用人单位获取个体同意, 也不现实。^① 对于求职者主动投递的简历信息, 应将其视为已向用人单位或招聘平台进行授权; 对于用人单位通过其他合法途径而获取的公开个人信息, 也不应要求用人单位对求职者再进行告知。如果做此类要求, 就会迫使企业与用人单位去更多获取个人联系信息以联系个人, 通过电邮或电话等方式骚扰个体, 这无疑会对求职者造成更大的侵扰。相比获取求职者的同意, 法律更应注重要求平台承担限期储存、及时删除、安全保障等责任, 此类信息的非法流转可能对个人造成难以预见的风险。^②

就权利适用而言, 根据上文提到的实用主义原则, 求职阶段的劳动者保护应更注重保障劳动者的消极性信息权利, 对包括招聘企业和网络招聘服务平台等信息处理者施加更多信息安全类义务。当企业或用人单位收集个人信息后, 个人应可以对其提起删除权、更正权、脱离自动化处理权等权利, 以确保自身信息的安全与准确。但对于个人提起的查询复制权、携带权等权利, 则应保持审慎。因为劳动者的个人信息往往以简历的方式存在, 包含了劳动者地址、电话、照片等全面信息, 申请者如果可以轻易获取此类信息, 可能反而对劳动者个人信息造成威胁。而就企业而言, 企业可以对劳动者信息进行合理规范的自动化处理, 以提高其招聘效率, 减少求职者不必要的面试, 但应严格履行限期储存、信息安全、反歧视等治理义务, 以避免算法决策与自动化处理给求职者带来的伤害。^③

值得提及的是, 面试阶段(包括电话面试)的劳动者个人信息保护与前期简历投递与筛选具有类似性, 在两种场景下, 劳动者与企业都未形成劳动关系, 且具有高度的信息共享需求。但二者不同之处在于, 简历投递与筛选阶段是在双方未形成密切关系的背景下的信息收集与利用, 双方关系仍然处于试探性阶段; 而面试阶段个人信息收集与利用更具有交互性, 双方对信息的真实性与质量要求更高。正如我国《劳动合同法》第8条规定: “用人单位招用劳动者时, 应当如实告知劳动者工作内容、工作条件、工作地点、职业危害、安全生产状况、劳动报酬, 以及劳动者要求了解的其他情况; 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。” 这类规定表明, 除非相关信息披露可能导致歧视或违反平等就业权等规定, 否则双方都负有更高的信息披露义务。更高的信息披露义务是双方信义关系开启的基础, 有利于和谐劳动关系的建构。

(二) 工作场所

一旦用人单位与劳动者建立劳动关系, 工作场所劳动者的个人信息保护将面临由劳动关系与信息关系所形成的双重支配问题。因此就法律适用而言, 此时需要适度突破隐私与个人信息保护的二元保护框架, 同时谨慎豁免小企业的个人信息收集与处理。对于一些不适用个人信息保护制度的劳动者隐私权保护问题, 也可以借鉴和援引个人信息保护制度, 或者采取其他法律制度进行应对。例

^① 2020年人社部出台的《网络招聘服务管理规定》第16条规定, “劳动者通过人力资源服务机构进行网络求职, 应当如实提供本人基本信息以及与应聘岗位相关的知识、技能、工作经历等情况”, 亦体现了对劳动力市场信息交换流通的支持立场。

^② 劳动关系非存续期间的个人信息处理, 参见谢增毅: 《职场个人信息处理的规制重点》, 载《法学》, 2021(10)。

^③ Aislinn Kelly-Lyth. “Challenging Biased Hiring Algorithms”. *Oxford Journal of Legal Studies*, 2021, 41(4): 900-905.

如一些企业可能要求其管理人员密切追踪员工，包括利用社交网络、搜索引擎实时关注员工状态。^① 此类行为虽然只属于隐私权而非个人信息保护法的管辖，但对员工无疑会造成巨大压力，增添用人单位与员工之间的不信任。为了应对此类行为，法律可以将个人信息保护法中对信息处理者的若干规制手段应用在此类行为中，以加强用人单位的隐私保护。

具体而言，劳动者隐私保护可以考虑借鉴《个人信息保护法》中有关合规审计、影响评估、隐私设计、安全保障义务等制度设计，例如对用人单位内部的隐私保护水平进行常规下的对照检查，对一些可能影响劳动者隐私的活动进行评估，在设计工作环境时更加注重隐私友好型的设计。^② 这些制度形式不一，但共通之处在于要求用人单位承担更高的隐私保护责任，而不仅仅是让实施劳动管理的个人一方承担隐私保护的所有责任。如果有的用人单位对侵犯隐私采取放任态度，甚至引入一些诸如“破冰文化”之类的陋习^③，此时应当通过执法检查与公益诉讼等方式对用人单位进行监管与诉讼，以弥补侵权法救济的不足。^④

就处理的合法性基础而言，用人单位可以根据人力资源条款或企业正当利益条款而在工作场所进行合理监控。因为此类监控有助于保护用人单位的有形财产与知识产权、提高生产率，也有利于保护员工财产、安全与免受骚扰，符合本文所提到的信义义务原则。但在此类工作场所监控中，应注重监控手段与实现目标、用人单位利益、个体利益与集体利益的协调。就监控手段与实现目标而言，监控手段应避免采取过于侵入型的方式，例如在采取视频监控与音频监控之间，应更多采取视频监控的方式，并进行醒目的提示。同时，应更多进行必要性和风险匹配性的监控，即将监控分布在那些实现相关利益极为必要，或者可能会产生重大财产、人身侵害风险的领域，避免采取过于侵入式（intrusive）的劳动监控。^⑤ 就相关群体的利益协调而言，应使相关监控在实现用人单位利益的同时，注重实现个体与集体的相关权益的平衡。借用前文关于信息信义义务的表述，用人单位在此类信息关系中不仅负有对个体的信义义务，而且对于集体也同样具有信义义务。用人单位应积极通过工会参与、集体协商等程序^⑥，构建和谐的工作场所监控环境，努力使工作场所监控成为强化各方信任的助推器，而非激化各方相互怀疑与担忧的离间者。

就具体权利义务适用而言，工作场所的个人信息保护应避免赋予个体绝对性的积极信息权利主张，但应赋予个体以消极性的信息权利^⑦以及加大用人单位的协商责任与信义法责任。这其中的原因在于，工作场所的个人信息保护至少涉及用人单位、劳动者个体、劳动者集体三方利益^⑧，同时还涉及企业人员之外的权益。在这种背景下，如果简单认同个体的积极信息权利主张，任由个体调

^① Sprague R. "Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship". *University of Louisville Law Review*, 2011, 50 (1): 1-34; Abril PS, Levin A and Del Riego A. "Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee". *American Business Law Journal*, 2012, 49 (1): 63-124.

^② “隐私设计”一直是个人信息保护中的重要一环，参见 Ira S. Rubinstein. "Regulating Privacy by Design". *Berkeley Technology Law Journal*, 2011, 26 (3): 1409-1456.

^③ 《互联网大厂“破冰文化”虚实》，参见 <http://www.cb.com.cn/index/show/jj/cv/cv12535134104>。

^④ 梁桂平：《劳资关系中劳动者个人信息权的法律救济》，载《重庆邮电大学学报》（社会科学版），2016（3）。

^⑤ Article 29 Working Party. Opinion 2/2017 on data processing at work (17/EN WP 249) (June 8, 2017), p. 7, <https://ec.europa.eu/newsroom/article29/items/610169>.

^⑥ 关于隐私与个人信息的集体保护，参见 Kim PT. "Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing". *Louisiana Law Review*, 2006, 66 (4): 1009-1034; Craver CB. "Privacy issues affecting employers, employees, and labor organizations". *Louisiana Law Review*, 2006, 66 (4): 1057-1077.

^⑦ 关于个人信息保护中的积极性权利与消极性权利，参见申卫星：《论个人信息权的构建及其体系化》，载《比较法研究》，2021（5）。

^⑧ 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（2）。

取、查阅、复制视频监控和混同个人与群体的信息、删除相关视频或混同信息，则用人单位与他人的相关权益就会受到很大威胁。但消极信息权利则不同，即使在公共空间，劳动者的消极性个人信息权利仍然非常重要。^①同时，用人单位由于要维护多方权益，其信息处理义务本身也具有协商和治理性质。^②例如有的男性员工可能希望收集的信息越少越好，有的女性员工则期望工作场所进行更多监控；有的员工可能希望所有收集的信息都能严格遵循限期储存，另外有的员工则希望此类信息能够保留更长时间。在这种背景下，简单遵循信息最小化原则或限期储存原则都难以调和各方利益。用人单位除了承担信息安全这类共识性较高的义务之外，还应有义务进行各方信息权益的协调。^③

（三）工作场所之外

传统劳动监控主要发生在工作场所之内，但随着现代科学技术的发展与应用，用人单位对劳动者工作场所之外的监控也开始大幅拓展。^④例如随着远程工作越来越普及，用人单位可能为劳动者提供访问软件、访问接口与视频对话，对劳动者的网络活动与工作情况进行监控。用人单位也可能为劳动者提供可穿戴设备，或者在公司车辆、户外劳动工具上安装定位，从而获取劳动者信息。^⑤此外，有的监控活动发生在物理上的工作场所内，但在信息技术与认知上却可以被视为工作场所之外。例如劳动者在工作单位用自带设备工作（bring your own device），劳动者可能在认知上将工作之外的场所视为个人生活自主的空间。^⑥

在劳动法传统制度如工伤认定规则中，工作场所内部发生的劳动者损害往往更容易寻求救济，而工作场所之外如出差途中、居家办公情形下的工伤认定劳动者则应承担额外的举证责任，包括对工作时间、广义工作场所和因工作原因受到事故伤害的证明。劳动者个人信息法律保护的逻辑与传统劳动法规则具有一定差异，由于涉及对劳动者私人空间的干涉，用人单位对工作场所之外的个人信息保护往往需要承担更严格的义务与责任。

就法律适用而言，对工作场所外的监控应同时适用隐私保护和个人信息保护。即使是小微企业，也不应豁免个人信息保护的适用。其原因有几点，一是此类工作外场所的监控通常通过科技手段进行，劳动者往往难以觉察；二是此类监控往往涉及劳动者工作与生活混同的场景，用人单位的监控很可能涉及劳动者的生活信息；^⑦三是劳动关系中固有的支配关系，将使得劳动者面临进一步遭受支配的风险，即使是少量收集个人信息的小微企业，当其通过技术手段获取劳动者的车辆行踪信息、网页浏览记录，也可能给劳动者带来巨大的威胁。因此，在此类场景下，小微企业也应履行

① 关于公共场所的隐私权，参见“磁场理论”或“气球理论”的分析，即个体在公共场所也应当有一个适度的个人空间，参见 Yanisky-Ravid S. “To Read Or Not to Read: Privacy within Social Networks, the Entitlement of Employees to a Virtual Private Zone, and the Balloon Theory”. *American University Law Review*, 2014, 64 (1): 53-108.

② 在比较法上，大陆法系相对更强调劳动者对于隐私的参与式治理，参见 Finkin MW. “Employee Privacy, American Values, and the Law”. *Chicago-Kent Law Review*, 1996, 72 (1): 221-270; Alan F. Westin. “Privacy in the Workplace: How Well Does American Law Reflect American Values”. *Stanford Law Review*, 2001, 53 (6): 1393-1462.

③ 社会协商制度作为解决劳动关系双方利益冲突，可参见林嘉：《劳动法视野下社会协商制度的构建》，载《法学家》，2016（3）。

④ 朱晓峰：《数字时代劳动者权利保护论》，载《浙江大学学报》（人文社会科学版），2020（1）。

⑤ Phoebe V. Moore. “Data subjects, digital surveillance, AI and the future of work”. available at [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU\(2020\)656305](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2020)656305).

⑥ Chris Brook. “The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits”. available at <https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating>.

⑦ Jeremias Adams-Prassl. “What if Your Boss Was an Algorithm? The Rise of Artificial Intelligence at Work”. *Comparative Labor Law & Policy Journal*, 2019, 41 (123): 16.

个人信息保护的一系列义务，例如对收集个人信息的情形进行告知，赋予劳动者一系列合理的信息权利，并承担信息处理者的信息安全与信息治理责任。

就合法性基础而言，工作场所外的监控应当更谨慎依赖人力资源管理或企业正当利益条款，而且此类监控应当特别注意最小必要性原则，避免将劳动监控推广到边沁与福柯笔下全景式监控的地步。^①例如在线下场景，有地区曾经环卫工人配发智能手环，一旦环卫工在原地不动超过了20分钟，这些智能手环就会进行提醒。此类做法就可能严重侵犯劳动者的权益。在线上场景，有的用人单位可能利用数据丢失预防（Data Loss Prevention）工具，预防企业数据泄露，或者利用防火墙、深度数据包检查（Deep Packet Inspection）等工具，对网站、内容进行过滤，追踪用户的身份信息与访问记录，此类行为也应当限于企业的风险预防所必需。一旦企业将这类工具用于获取用户的非工作信息，或者采取太过宽泛的信息收集与预防措施，这类行为就可能超出必要选原则。^②此外，在所有此类监控中，用人单位也必须对劳动者进行明确告知和清晰的警示。对于劳动者因为不知情而导致的个人信息被秘密收集、处理和泄露，个人既可以通过隐私权而提起诉讼，也可以通过个人信息保护的过错推定原则而提起侵权之诉。^③

就权利义务适用而言，工作场所外的劳动者应对其单独被收集的各类信息具有较为广泛的信息权利，但对于混同他人的信息则不应享有此类权利。例如当劳动者在家远程工作，或者使用自带电脑进行工作，此时对于用人单位所收集的只包含某个个体的信息，劳动者应有权利通过知情权、查询复制权、更正权、删除权等权利而维护自身权益，同时对用人单位的信息收集与处理行为进行制约。但如果个人使用的是企业设备或车辆，此类设备上混同了用人单位其他劳动者的信息，则此时劳动者的某些信息权利主张就可能威胁其他劳动者。劳动者应享有对其信息是否被收集的知情权，但不应具备查询复制权、携带权等权利。

用人单位应对工作场所外的劳动者信息保护承担更高的信义义务。除了在某些场景下的职业安全保护需要，^④工作场所外的信息收集必要性相对较低，最主要涉及用人单位的利益，与劳动者个体与集体权益的相关性较低；同时，由于工作场所外劳动者的工作信息与生活信息往往高度融合，因此用人单位应当在目的限制、信息最小化、限期储存、信息安全、信息质量等方面设置更高的标准，以最大程度降低现代科技对劳动者带来的侵扰与威胁。^⑤用人单位以更高标准和更少侵入性地方法保护工作场所外的劳动者个人信息，不但对于保护劳动者至关重要，对于建立劳动者对于用人单位的信任，构建和谐劳资关系与企业氛围，也具有重要意义。

本部分所讨论制度设计不仅适用于劳动关系场景，还可应用于劳务派遣、共享用工等多元用工关系，根据用工主体处理个人信息之具体情形施以隐私或个人信息保护责任。如在劳务派遣关系中，派遣单位与劳动者签订劳动合同，派遣单位应履行求职环节和日常人力资源管理环节对劳动者的隐私和个人信息保护义务，而实际用工单位则应注重承担工作场所内的协商责任和信义法责任

^① Lilian Edwards, Laura Martin and Tristan Henderson. "Employee Surveillance: The Road to Surveillance is Paved with Good Intentions". available at https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/17297/edwards_lecture_capture_final.pdf?sequence=1.

^② Lilian Edwards, Laura Martin and Tristan Henderson. "Employee Surveillance: The Road to Surveillance is Paved with Good Intentions". available at https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/17297/edwards_lecture_capture_final.pdf?sequence=1.

^③ 《民法典》第1032、1033条；《个人信息保护法》第69条。

^④ 相关分析，参见班小辉：《远程工作形态下职业安全保护制度的困境与应对》，载《甘肃政法学院学报》，2019（5）。

^⑤ Secunda PM. "The Employee Right to Disconnect". *Notre Dame Journal of International & Comparative Law*, 2019, 9 (1): 1-39.

等。对于争议较大的新就业形态，如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平台用工的情形，^① 尽管从劳动关系认定结论看其尚未具有典型劳动关系的从属性程度，但由于平台与从业者之间依然具有一定的控制、支配关系，此类新型用工关系的处理仍可参照劳动者个人信息法律保护进行制度设计。如就在线劳动平台处理个人信息的正当性基础问题，应参照消费者个人信息保护场景，要求平台履行一般的告知同意义务。由于平台与从业者之间一定程度的支配关系，从业者往往面临必须同意平台各项信息处理行为的处境，因此，应要求平台积极承担信义义务责任，不得利用所收集信息进行算法剥削或算法歧视等不当行为。^② 在敏感个人信息处理的问题上，则应限制“同意”作为处理行为合法依据的效力，以“合同所必需”作为处理从业者个人信息的前提，并向从业者告知处理敏感个人信息的必要性以及对个人权益的影响。^③

五、结语

个人信息保护与劳动者保护具有很高的相似性。二者所保护的关系都具有一定的持续性不平等特征，且双方既具有合作性，又具有一定的支配性和防范性。在个人信息保护中，个人信息的合理共享有利于双方更了解彼此，从而促进双方的共同利益；也可能导致信息处理者对个体的支配与操控。在劳动关系中，用人单位与劳动者之间亦然，既可能形成彼此互惠互利的良性关系，也可能导致用人单位对个人权益的侵犯。同时，个人信息保护与劳动者保护还采取了类似的法律结构，例如一方面都对个体或劳动者进行赋权，另一方面则对信息处理者与用人单位施加责任。二者都采取了一种合作治理的法律框架。^④

由于个人信息保护与劳动者保护的这些特征，这二者本身就面临很多争议。例如个人信息保护研究中，就存在个人信息保护法益的不确定性、场景依赖性、制度弹性等问题。在劳动保护中，也长期存在更多强调市场自治与劳动规制的讨论，劳动法所确立的各项制度也面临刚性程度不一的问题。当个人信息保护问题与劳动者保护问题叠加，其中所存在的问题就被叠加，甚至更进一步放大了。

本文分析了劳动者个人信息保护的若干核心挑战，例如其法律适用问题，其保护应当适用隐私侵权的框架还是个人信息保护法的框架？是否应当对小微企业进行个人信息保护的豁免？个人信息处理的合法性基础是否应该有所不同？劳动者个人信息保护是否应当适用个人信息保护中的一般权利与义务？经过原理层面的反思，本文认为，应当以信息信义义务与实用主义的原则指导劳动者个人信息保护，在此基础上分场景构建具体制度。^⑤ 综合而言，用人单位应当承担更高的企业治理义务，在兼顾企业正当利益的同时应当创造良好的隐私与个人信息保护环境，让个人信息的合理收集与处理成为促进劳动者个体与集体信任的工具。如此，劳动者个人信息保护就可能实现劳动者保护与个人信息保护的双赢。

^① 《关于维护新就业形态劳动者劳动保障权益的指导意见》，参见 http://www.mohrss.gov.cn//xxgk2020/fdzdgknr/zcfg/gfxwj/ldgx/202107/t20210722_419091.html。

^② Calo R and Rosenblat A. "The Taking Economy: Uber, Information, and Power". *Columbia Law Review*, 2017, 117 (6): 1623.

^③ 将个人信息划分为敏感个人信息和一般个人信息，对敏感个人信息予以特殊保护的观点可参见张新宝：《论个人信息权益的构造》，载《中外法学》，2021（5）。

^④ Kaminski ME. "Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability". *Southern California Law Review*, 2019, 92 (6): 1529 - 1616.

^⑤ 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（8）。

On The Challenge and Response of Legal Protection of Workers' Personal Information

DING Xiaodong

(School of Law, Renmin University of China)

Abstract: The protection of workers' personal information faces challenges such as the application of privacy and personal information protection, the legitimacy basis of personal information processing, and the uncertainty of specific rights and obligations. The reason is that the protection of personal information and the protection of workers are both asymmetric unequal relations, and their relations are both cooperative and antagonistic. The superposition of the two problems makes the personal information protection can not simply adopt the framework of general personal information protection. We should adopt the principles of fiduciary duty and pragmatism, take into account the legitimate interests of employers, require employers to bear the responsibility of personal information management of enterprises, and provide safe and reliable personal information collection and processing for individual and collective workers. In terms of system, the relevant systems of personal information protection should be applied according to different scenarios to achieve the dual objectives of personal information protection and worker protection.

Key words: labor protection; unequal; personal information; fiduciary duty; pragmatism