用人单位知情权与劳动者隐私权冲突的解决路径

宋慧灵

温州大学，浙江温州，325035；

摘要：本篇文章深入分析了用人单位知情权与劳动者隐私权之间的冲突及其解决路径。随着社会的发展，劳动关系日益复杂，用人单位出于管理需要和风险防范考虑，对劳动者个人信息的需求不断增加。然而，这种需求的出现常常与劳动者的隐私权产生冲突，尤其是在大数据背景下，显得更加突出。本文首先剖析了用人单位知情权和劳动者隐私权的法律基础及其内涵，阐述了两种权利冲突的主要表现形式。其次，对两者冲突产生的根源进行了分析。在此基础上，本文提出了解决用人单位知情权与劳动者隐私权冲突的路径：建立以场景理论为基础的隐私动态评估模型、优化劳动者“知情同意”制度、打造集“预防、监管、问责”功能于一身的算法风险管理架构、构建多方合作的员工隐私防护体系。最后，文章强调了在保障用人单位合法权益的同时，应当更加注重劳动者隐私权的保护，以促进劳动关系的和谐稳定发展。

关键词：用人单位知情权；劳动者隐私权；权利冲突；信息保护

DOI：10.69979/3029-2700.24.5.013

引言

在目前数字化技术迅猛推进的背景下，用人单位知情权与劳动者隐私权之间的冲突日益凸显，成为劳动法领域的一个重要议题。随着劳动关系的复杂化和信息技术的进步，用人单位出于管理需要和风险防范考虑，对劳动者个人信息的需求不断增加。然而，这种需求与劳动者隐私权的保护之间常常存在张力。本研究旨在探讨这一冲突的根源、表现形式以及可能的解决路径，以期在保障用人单位合法权益的同时，更好地保护劳动者的隐私权。依据中华人民共和国人力资源和社会保障部发布的数据，在 2021 年年末，全国就业总人数攀升至 7.46 亿，在此之中，城镇地区的就业人数为 4.67 亿。在这庞大的劳动力市场中，平衡用人单位知情权与劳动者隐私权的重要性不言而喻。本文旨在阐述两种权利冲突的主要表现形式，分析冲突产生的根源，提出针对性的应对策略，从而平衡用人单位知情权与劳动者隐私权，推动劳动关系的协调与平稳发展。

1 用人单位知情权与劳动者隐私权的冲突现状

1.1 用人单位知情权的内涵和法律依据

用人单位知情权是指用人单位在劳动关系中，为了合法行使管理职能与完成法律所规定的职责，拥有掌握与劳动者有关的必要信息的权利。这一权利的法律依据主要源于《劳动合同法》、《劳动法》等相关法律法规。例如，《劳动合同法》第八条明确指出，雇主有权掌握与劳动合同直接相关的基本信息，雇员必须如实陈述。

在实际操作过程中，关于用人单位知情权的界限和限度的争议屡见不鲜。一些用人单位倾向于广泛收集劳动者的个人信息，包括健康状况、家庭背景、信用记录等，此类行为常常逾越了法律所界定的必要限度。根据中国互联网协会发布的《中国互联网发展报告 2021》，超过六成的的企业在招聘环节中会对求职者的社交媒体信息进行收集，这一做法引发了对劳动者隐私权保护的担忧。

1.2 劳动者隐私权的概念和保护范围

劳动者隐私权指的是在工作关系建立、维持、结束的各个阶段，员工根据法律享有的个人生活平静不被雇主干扰、个人空间不被雇主闯入、个人活动不被雇主影响以及个人信息不被雇主侵犯的权利。这一权利的法律基础包括《宪法》、《民法典》等法律中关于公民隐私权的规定。《民法典》第一千零三十二条清晰地规定了自然人拥有隐私权，禁止任何组织或个人通过窥探、干扰、泄露或公开等手段侵犯个人的隐私权。

劳动者隐私权的保护范围通常包括个人身份信息、通信记录、健康状况、家庭情况等。随着技术的发展，这一范围还在不断扩大，如生物特征信息、位置信息等。据中国互联网络信息中心（CNNIC）的统计，截至 2021 年底，我国网民人数已增长至 10.32 亿，网络普及率达到了 73.0%。在这样的环境下，确保劳动者的数字隐私安全显得尤为关键。

1.3 两种权利冲突的表现形式

用人单位知情权与劳动者隐私权的冲突主要表现在以下几个阶段：

1.3.1 劳动关系缔结阶段：过度收集及不恰当的筛选劳动者私密信息

依据我国《劳动合同法》第八条，雇主有权掌握与劳动合同直接相关的基本资料，而雇员必须如实提供这些信息。此条款为雇主合法获取雇员个人信息（包括部分私密信息）奠定了基础。从理论上讲，根据与工作职位的关联性，雇员个人信息可以分为三类：(1)与工作职位紧密相关、直接作用于工作能力和职责执行的信息，例如年龄、教育背景等；(2)与工作职位间接相关、但可能在将来影响工作能力和职责执行的信息，如基本健康状况等；(3)与工作职位无关、未来不会影响工作能力和职责执行的信息，例如宗教信仰等。当然，同种个人信息对于不同职业岗位，可能归于不同的类型。

在大数据时代背景下，数字技术的快速进步降低了用人单位在收集、存储、传递劳动者信息时的经济成本，同时效率显著提升。在用人单位的“知情权”和信息主体的“同意规则”保护下，为了达到“择优录用”的目标，用人单位在招聘时可能会要求求职者提供超出常规范围的个人信息（求职者为了获得理想职位，往往愿意满足用人单位的所有信息要求，哪怕这些信息是私密的）。此外，用人单位也可能通过主动与第三方合作，全面搜集候选人的个人信息。

另一方面，在建立劳动关系的过程中，用人单位经常利用大数据分析技术，对求职者的个人信息进行筛选。筛选的标准不仅限于年龄、教育背景、性别、婚姻状况、专业技能、个性特点、健康状况以及奖惩记录等众多指标。有些公司甚至考虑性格评估、血型、星座等元素，以此来判断求职者是否与企业文化匹配，进而决定是否雇佣该求职者以及其未来的工作环境和薪酬福利。此类操作不仅导致了待遇差异和数据偏见，同时也加深了对劳动者隐私的侵犯风险。

1.3.2 劳动关系存续阶段：该阶段是用人单位知情权与劳动者隐私权发生冲突的主要阶段，在数字技术支持下，主要表现在如下方面：

（1）过度监视劳动者私密活动。在工作活动中，员工的行为大致可以划分为职业行为与个人行为；雇主作为劳动力成本的承担者，期望劳动力效益最大化，因此倾向于减少员工的个人行为。在信息时代，雇主对员工行为的监控成本显著降低，这导致员工私生活受到干扰的可能性大幅上升。例如，南京的环卫工人被要求佩戴智能手环以便于工作安排，一旦休息超过 20 分钟就会响起“加油”警报，并且其行动路径会受到精确追踪，一旦工作时间离开指定区域，系统就会记录处罚信息。更进一步，一些雇主采取隐蔽手段对员工进行监控和监听，比如某企业以关心员工健康为名提供高科技坐垫，用以收集员工的生物健康信息，但管理层却利用这些数据监控员工，通过算法判断是否有偷懒行为。

（2）肆意侵扰劳动者私密空间。在大数据时代背景下，一方面，工作场所的界限逐渐变得不那么明显。例如，借助信息技术的居家办公，使得工作与个人生活逐渐融合；平台用工在算法的操控下，导致了工作者的办公环境变得虚拟和流动。另一方面，个人领域的界限正逐渐扩展。在数字化时代背景下，工作者的个人领域不仅涵盖了具有实体的个人工作地点、私人物品储藏空间、私人信件以及身体隐私，还扩展到了电子邮箱、微信、QQ、社交圈、微博、云存储等数字化平台。这些变化在重新塑造工作环境和流程的同时，也给工作者的隐私权带来了新的威胁。无论是在国内还是国外，远程工作的工作者们经常面临雇主收集和监控个人信息的情况。利用算法技术，雇主能够对远程工作者的工作行为和状态进行全时段的实时监控。这种做法对工作者的个人隐私、人格尊严以及自由构成了前所未有的挑战。

（3）暴露劳动者隐私于算法系统之中。在大数据的背景下，算法管理成为了用人单位在劳动管理方面的新趋势，特别是对于网络平台公司来说。算法管理在劳动管理中的核心是运用算法构建的“规则集”来执行自动化的决策流程，并且不断地对员工的行为进行规范化的引导，旨在提升企业的运营效率。因此，用人单位不仅持续收集员工的工作时间和地点的个人数据，还不断收集员工在工作时间和地点以外的个人信息，这已超出公司员工管理的界限，侵犯了员工的隐私权。举例来说，一些雇主采用计算机活动监控技术，导致人力资源部门的后期审查转变为监控软件的即时审查、自动分析。

1.3.3 劳动关系终止阶段：消极泄漏与积极转移劳动者隐私信息。

在这一时期，劳动者隐私权受损主要因为雇主对个人（隐私）资料的被动泄露和主动传递，这包括未能妥善执行安全保护措施，造成资料意外泄露，以及故意将资料非法出售给第三方等行为。例如，雇主在员工离职后，将他们的个人信息卖给招聘网站或人力资源公司以谋取利益的情况并不少见。需要强调的是，这种非法交易个人信息的行为不仅在劳动关系结束时发生，在劳动关系的建立和维持期间也可能出现。实际上，在劳动关系结束时，雇主掌握的隐私信息更多，对隐私权的侵犯也更加严重。此外，雇主向第三方出售劳动者信息后，第三方又将这些信息转卖给其他公司的现象也相当普遍。

2 冲突的根源分析

2.1 法律规定的模糊性和不完善

用人单位的知情权与劳动者隐私权之间的矛盾，很大程度上源于现行法律规定的不明确和不完整。尽管我

国已经出台了一系列旨在保护个人信息和隐私权的法律，包括《民法典》和《网络安全法》等，但在劳动关系领域，针对用人单位知情权和劳动者隐私权的规定尚处于模糊地带，缺乏具体细化。

例如，《劳动合同法》规定了雇主有权掌握雇员的相关信息，但未明确“相关情况”的具体界限。这使得在实际操作中，雇主常常倾向于广泛搜集雇员资料，而雇员却难以分辨哪些信息是必须披露的。据中国政法大学劳动法与社会保障法研究所的一项调查，超过七成的受访雇员反映曾遭受雇主过度搜集个人信息的情形。

2.2 社会环境和技术发展带来的新挑战

在当前社会背景下，社会环境日益变化，技术发展不断迭代，大数据、人工智能等新技术的应用使得信息收集和分析变得更加容易，从而让用人单位了解和监控劳动者变得更加便利，导致用人单位知情权与劳动者隐私权的冲突更为凸显。例如，面部识别技术的广泛应用使得用人单位可以更精确地监控员工的工作时间和行为。

同时，社交媒体的普及也使得个人隐私边界变得模糊。许多用人单位会通过查看求职者或员工的社交媒体账号来获取额外信息。据麦肯锡全球研究院的报告显示，全球有 70%的招聘者会利用社交媒体筛选候选人。这种做法虽然可以帮助用人单位更全面地了解求职者，但也可能侵犯个人隐私权。

2.3 用人单位与劳动者之间的不对等

用人单位与劳动者之间存在的权利不对等是导致知情权与隐私权冲突的另一个重要原因。当劳动力供应超出市场需求时，劳动者常常处于相对弱势地位。为获得或保住工作机会，许多劳动者不得不接受用人单位提出的各种要求，包括提供个人隐私信息。

根据中国劳动关系学院的一项研究，有超过 60%的劳动者表示，即使认为用人单位的某些做法可能侵犯隐私，也不敢明确拒绝或提出异议。由于权利的失衡，用人单位有可能不合理利用信息优势，导致对劳动者的隐私权维护变得异常艰难。特别是在一些新兴行业和灵活就业形态中，这种不对等更为明显。例如，在网约车、外卖配送等平台经济领域，平台公司往往掌握大量关于劳动者的个人信息和工作数据，而劳动者对此几乎没有控制权。

3 解决路径的探索

3.1 建立以场景理论为基础的隐私动态评估模型

在静态隐私认定失灵的背景下，尼森鲍姆(Nissenbaum)提出了“隐私场景一致性理论”(Contextual integrity Theory)，主张个人信息保护应考虑具体场景，对信息收集者施加不同的限制。在不同场景中，信息主体、处理者和传播环境的交汇会导致隐私期望和潜在危害的层次差异；因此，评估隐私保护的合理性，必须依据具体情境进行。在特定情境下，个人数据可能仅仅是普通信息，但当环境改变，这些信息可能就变成了隐私。例如，家庭成员和朋友间共享的住址信息，在陌生人面前就可能被视为私密。个人信息的识别度也会随着环境的不同而有所改变。所以，判断一个信息是否应受隐私保护，并非仅看其是否容易被识别，而是要基于信息主体对隐私的合理期望，并结合该信息在特定情境下可能遭遇的隐私风险，动态地确定其隐私属性。在评估合理隐私期望时，应采用主观和客观相结合的双重标准。一方面，这关乎个体是否在主观上表现出对隐私的真正期望。另一方面，在客观层面，社会公众是否认为这种隐私期望是合理的。例如，非法信息不享有隐私，隐私权不能与公共安全利益相抗衡。

回归到劳动关系中，在遵循场景隐私理念的框架内，雇主在进行劳动管理时，对员工的隐私信息进行合理限制和使用，需要考虑的因素可以分为四个层次：首先是必须遵守的基本原则；其次是员工对于隐私的合理期待；第三是针对员工隐私限制或使用具体情境的考量，这包括了目的、范围、方法、程序和组织措施等方面；最后是对于不合理的限制和使用可能带来的隐私风险。

3.2 优化劳动者“知情同意”制度

一些学者提出，知情同意原则实际上并不能有效地维护个人隐私权益，反而可能阻碍大数据领域的发展；他们认为，知情同意原则并非不可或缺，应让位于信息共享和经济增长。本文认为，尽管知情同意原则在实施效果上不尽人意，其制度构建初衷是为了保障权利人能够预先将个人隐私信息的风险限制在期望的限度内。个人尊严不应屈从于商业利益，即便在有效性方面存在不足，也不应否定其存在的价值。此外，在劳动领域，若放弃知情同意原则，将等同于对员工权益的侵害，这将加剧雇主与雇员之间权利的不平衡。我们应当针对实际情况对其进行优化，以应对大数据时代带来的新挑战，寻求经济发展与隐私权保护之间的平衡，并且将信息自主权作为核心原则。

在劳资关系中，雇主的信息索取与控制权与雇员的隐私保护之间存在一种此起彼伏的关系。在各种不同的情境下，雇员对隐私的期望也有所差异，不能简单地将所有个人隐私信息以同一情境标准来处理。必须放弃以往那种一概而论的同意方式，将情境机制融入知情同意的规则里，依据情境风险对同意的程度进行区分，实施

“两端加强”的策略，达成一致的层次划分，这更符合劳动者的实际状况，同时也能调和无差别同意原则所导致的不平衡。

具体而言，首次授权时，在低风险情境中，应重视效率价值。在这些情况下，应尽量减少不必要的告知和同意，避免造成同意疲劳。默示同意相较于明示同意，能显著节省时间和金钱，同时提升信息传递速度。因此，低风险情境适合采用默示同意。尽管如此，优先采用默示同意并不意味着剥夺劳动者的撤回权，他们依然保有这一权利，这有助于保护劳动者的自主性并提高规则的灵活性。高风险情境可能严重威胁劳动者隐私，此时应重视安全价值。除了采用明示同意外，还应要求逐项同意，并设置前置程序。即在劳动者同意之前，政府监管机构需对用人单位的信息收集行为进行更严格的评估。对于不合理或不必要的收集行为，应加以限制或调整，并将评估结果通报给劳动者，以便他们做出是否同意的决定。中风险情境应在安全与效率之间寻求平衡，明示同意足以保护劳动者的权益；若要求像高风险情境那样进行二次风险评估和限制用人单位，将给用人单位带来过重的负担，降低信息流通效率，得不偿失。

在二次或多次授权同意的情况下，必须判断是否与初次授权处于相同的风险环境，并且是否满足劳动者的合理期望。若风险等级未变且满足劳动者对隐私的期望，则无需劳动者再次授权，也不必重新评估风险；若风险等级改变或不符合信息主体的合理期望，则应如同初次授权时那样重新进行初步风险评估，并根据评估结果采取适当措施。这样可以显著提升各方的效率：用人单位在收集、处理、传递个人信息方面的成本将大幅减少，同时劳动者在个人信息管理上的时间成本也会显著降低，确保了劳动者对个人信息的自主控制权和对隐私的合理期望。

3.3 打造集“预防、监管、问责”功能于一身的算法风险管理架构

在大数据的浪潮中，构建一个全面的算法风险管理框架显然是预防隐私泄露风险的根本措施。安·卡沃基安(Ann Cavoukian)倡导了“通过技术设计来保护隐私”的理念（简称“PbD”），其主要观点有二：首先，主动防范风险，将价值和设计原则融入产品开发的初始阶段，并辅以事后的补救措施；其次，确保产品在出厂时默认设置旨在保护用户的个人信息。算法的伦理取向由其开发者决定；一旦开始应用，这些伦理取向可能会对工作者的隐私安全造成影响。因此，算法开发者的决策不仅影响个人，还会对整个社会工作者的隐私保护产生影响。从这个角度来看，算法开发者就像生物遗传学中的“基因捐献者”；因此，算法开发者应对算法运行中可能引发的工作者隐私风险负有“产品质量责任”。具体来说：

1.构建一个以“算法伦理指引”为核心的预防体系至关重要。在开发算法产品时，算法生产者必须主动融入积极的伦理价值观。2021 年 9 月 25 日，国家新一代人工智能治理专业委员会发布了《新一代人工智能伦理规范》（简称《伦理规范》），旨在将伦理道德理念融入人工智能发展的每个阶段，引导所有涉及人工智能的个人、企业和其他相关实体遵守伦理原则。因此，算法生产者应遵循《伦理规范》的规定，承担起预防算法伦理风险的责任，并且有权拒绝执行违背算法伦理的管理或委托要求。

2.以“算法备案管理”为关键的算法监管体系得到了加强。自 2022 年 3 月 1 日起，我国国家互联网信息办公室（简称“网信办”）、工业和信息化部、公安部以及国家市场监督管理总局联合颁布的《互联网信息服务算法推荐管理规定》（简称《算法管理规定》）开始正式实施。在这一规定中，算法备案管理得到了具体实施。算法备案管理构成了我国监管体系的关键部分。在算法产品投入市场前，备案主体需要遵守《算法管理规定》的条款，通过“互联网信息服务算法备案系统”完成备案流程，并提供算法主体、产品及其功能、算法细节等详尽信息。展望未来，国家算法监管机构应进一步明确“社会动员能力”的主体界定标准，并推广“告知备案”流程，以明确备案的界限。

3.需建立以“责任主体问责”为核心的算法责任体系。结合《伦理守则》与《算法治理条例》的相应条款，依照国家法律、法规的基本原则，通过法规、规章等规范性文件，界定算法侵犯劳动者隐私权等不良后果出现时，算法开发者和使用者应承担的法律责任，并确保受损方能够顺利获得权利救济。

3.4 构建多方的员工隐私防护体系。

1.确保在劳动执法监察过程中，对劳动者隐私权的保护得到明确。通常情况下，劳动者在劳动关系存续期间不会主动维护自己的隐私权；一旦隐私权受到侵害再去维权，往往代价高昂且效果有限。劳动执法监察是维护劳动者权益的有效手段。为了让劳动者更有底气，应当扩展劳动执法监察的职责范围，将劳动者隐私权保护纳入基准法，并将其作为政府劳动监管部门常规检查的一部分；必须明确劳动执法监督机构在保护劳动者隐私安全方面的职责，改善举报和投诉流程，迅速制止用人单位对员工隐私权的侵犯行为。

2.工会在保护劳动者隐私权方面发挥着独特作用。

作为劳动者的“后盾”，在捍卫权益方面，工会相较于劳动者本人和其他社会团体，拥有明显的优势，包括在利益表达、救济途径和保护强度等方面。在数字化时代背景下，工会必须持续提高其数字能力与技术，通过教育劳动者关于隐私权保护的知识、推动集体谈判、签订集体协议等多种方式，主动引导劳动者与雇主就隐私权保护等议题达成共识，明确双方的权利与义务，促进雇主的知情权和劳动者的隐私权之间的和谐共处和平衡发展。

3. 强调用人单位在维护劳动者隐私权方面的主导角色。用人单位在维护劳动者隐私权上，不仅负有首要责任，也是最直接的义务承担者，同时可能成为隐私权侵犯的源头。在大数据时代背景下，确保用人单位在劳动者隐私权保护上的主导地位，除了要持续强化其在传统技术环境下对劳动者隐私的保护职责外，还应特别关注“个人信息合规审计”和“个人信息保护负责人”制度的实施。根据我国《个人信用信息保护法》第 54 条，已规定了个人信息处理活动的内部合规审计制度；2021 年 12 月 6 日，“个人信息保护合规审计推进小组”发布了《关于推进个人信息保护合规审计的若干建议》（简称《建议》），该《建议》基于现行的个人信息保护法规，为个人信息从产生到销毁的各个阶段提供了合规审计的具体指导。因此，用人单位必须依照《个信法》和《建议》所规定的内容和要求，明确识别劳动者隐私风险和安全事件信息的来源，准确掌握风险评估和安全事件识别的相关因素，执行个人信息处理活动的内部合规审计。同时，为了确保“个人信息保护负责人”制度的实施与细化，用人单位应遵循《个人信息保护法》和《信息安全技术个人信息安全规范》（GB/T 35273-2020）的要求，通过内部制度明确个人信息保护负责人的职位保障、职责范围和责任追究等具体条款。对于那些尚未满足设立个人信息保护负责人条件的用人单位，可以通过制定内部规章，让企业人事管理部门的负责人或法定代表人承担个人信息保护的职责，从而增强企业对劳动者隐私信息管理的力度和保护水平。

4 结论

在劳动关系的处理过程中，如何平衡用人单位知情权与劳动者隐私权的冲突是一个重要议题，这要求各方面共同努力，探索解决的途径。本文提出的解决路径包括建立以场景理论为基础的隐私动态评估模型、优化劳动者“知情同意”制度、打造集“预防、监管、问责”功能于一身的算法风险管理架构、构建多方合作的员工隐私防护体系。为实现这些措施，政府、企业、社会组织及个人必须携手合作。在将来的发展道路上，我们应在确保雇主权益的基础上，进一步强化对员工隐私权的保护，以满足信息时代的要求，并推动劳动关系的和谐与稳定进步。只有法律、制度和文化等多方面共同努力，才能有效地建立一个长期保护员工隐私权的体系，达成用人单位与劳动者权益的均衡。

参考文献

[1]汤晓莹. 数字时代下劳动者离线权的证成与实现[J]. 河南财经政法大学学报，2024，39(02)：60-70.
[2]宋保振. 社会权视阈下“数字弱势群体”权益保障[J]. 法学，2024，(01)：20-34.
[3]王霞，鄢志文. 数字经济下新业态劳动者隐私权保护困境反思与进路构建[J]. 齐齐哈尔大学学报(哲学社会科学版)，2023，(10)：117-121.
[4]张耀文. 比例原则在雇员个人信息保护中的构造及适用[J]. 交大法学，2023，(06)：158-172.
[5]刘俊宜，钟邓鹏，李毅. 公法视域下的劳动者个人信息保护——以保障劳动者知情同意权为研究视角[J]. 中国劳动关系学院学报，2023，37(05)：61-71.
[6]冉克平，刘冰洋. 人力资源管理中个人信息保护的困境与出路[J]. 华中科技大学学报(社会科学版)，2023，37(04)：61-73.
[7]王东方. 职场电子监控的法律规制——以比例原则为核心的分析[J]. 东北大学学报(社会科学版)，2023，25(03)：116-123.
[8]徐强胜，王萍萍. 论职场智能监控与劳动者个人信息保护之边界[J]. 湖北社会科学，2023，(03)：121-129.
[9]韩笑；. 职场视频监控的法律规制——以劳动者隐私权保护为中心[J]. 湖北科技学院学报，2023(01)：59-65+96.
[10]江晓君. 数字化时代背景下劳动者个人信息保护研究[J]. 市场周刊，2022(10)：178-181.
[11]邹开亮；丁稳；. 大数据时代劳动者隐私权保护路径构造[J]. 价格理论与实践，2022(10)：62-67+214.
作者信息：宋慧灵（1999），女，汉族，四川省岳池县，温州大学硕士研究生，研究方向法学（民商法学）.