功利主义视角下个人数据信息利用与保护的平衡研究

蒲世豪

西南民族大学法学院，四川 成都 610041

摘　要：本文运用功利主义伦理框架，探讨数字时代个人数据信息利用与保护的平衡。文章首先阐述功利主义“最大多数人最大幸福”的核心原则，并分析了数据利用在经济、公共安全及社会服务中与个人隐私权的冲突。为解决此矛盾，文章提出法律与社会层面的策略：法律上，通过利益计算构建趋利避害的制度并强化监管；社会上，通过教育和行业自律培育道德自觉。其最终目标是构建一个能最大化社会福祉，既释放数据价值又保障个人权利的公正数据治理体系。

关键词：功利主义；个人数据信息保护

DOI：10.64649/yh.shygl.2025020011

0 引言

“个人信息”的核心在于其“可识别性”，即能够单独或结合其他信息识别特定个人的信息总和。在网络环境中，“个人数据信息”这一概念更侧重于其电子化与网络化特征，涵盖了从身份信息到网络活动轨迹的广泛数据。随着大数据与人工智能技术的发展，其种类和数量激增，对个人信息保护提出了严峻挑战。面对数据利用带来的巨大社会价值与个人隐私泄露风险之间的紧张关系，如何在保障个人权利的同时促进社会整体福祉，成为一个亟待解决的议题。

1 功利主义理论

功利主义（Utilitarianism）是伦理学史上影响深远的思潮，它为评估社会政策与法律提供了核心的决策框架：任何行为、法律或政策的最终目标，都应是实现“最大多数人的最大幸福”。该理论的集大成者杰里米·边沁（Jeremy Bentham）认为，人类天性是追求快乐、规避痛苦，因此一个行为的道德价值取决于其后果——即它能在多大程度上增加相关者的快乐并减少其痛苦。这种以理性计算为核心的道德决策模式，要求社会在面临选择时，权衡不同方案的后果，选择那个能够实现最大幸福总量的方案。边沁将“法律”视为实现这一目标的关键工具，其核心功能是通过调节社会秩序，化解冲突、遏制自私，为社会道德提供制度性保障。边沁甚至试图将此伦理学变为一门精确的科学，提出了“幸福计算法”（Felicific Calculus）。他主张在衡量行为后果时，应系统考量快乐或痛苦的强度、持续时间、确定性、邻近性、衍生性及纯粹性等多个维度，并将其影响的人数纳入计算。这种量化分析的思路，为现代政策制定中的成本效益分析提供了理论雏形。在边沁看来，脱离了功利计算的所谓“自然权利”是“踩着高跷的胡言乱语”，只有那些能实际增进社会总幸福的权利才具有真正的价值。

约翰·斯图亚特·穆勒（John Stuart Mill）在功利主义的框架内，将个人自由与自我发展置于实现全面幸福的核心。他认为，真正的幸福不仅是外在条件的满足，更是个人内在精神层面的自由成长。因此，保障个人自由是通往幸福的必由之路。但这种自由并非绝对，其核心边界是“伤害原则”（Harm Principle）：任何人的行为自由，以不损害他人的利益为限。社会对个人自由的干预，其唯一正当的目的就是防止对他人造成伤害。此外，穆勒补充了边沁的外在惩罚理论，强调仅靠法律等外部制裁不足以塑造道德社会，源于内心自觉的“良心”才是功利原则的终极保障。他认为，这种内在的道德动力，是可以通过后天教育和社会影响培养而成的。穆勒还对幸福的内涵进行了深化，认为幸福不仅有量的区别，更有质的高下之分。他著名地论断：“做一个不满足的人，胜于做一只满足的猪。”他主张，运用人类更高官能所获得的“高级快乐”，本质上优于纯粹的感官满足。这种对幸福质量的强调，将个人发展与个性表达的重要性提升到新的高度，也意味着保护个人自由与隐私，不仅是为了避免直接的物质或精神伤害，更是为了给个体追求和实现这些高级幸福提供必要的空间与尊重[1]。

这些功利主义的核心思想——边沁的后果计算与穆勒对个人自由和高级幸福的强调——共同为我们审视个人数据利用与保护的冲突，提供了一个旨在平衡社会整体利益与个体长期发展的伦理罗盘。

2 个人数据信息的冲突

2.1 网络经济发展与个人信息权益的冲突

数字经济的蓬勃发展，使得个人数据信息成为商业竞争的核心资源，其巨大的商业价值驱动着企业以前所未有的广度和深度进行数据挖掘，从而引发了其与个人信息权益之间一系

列深刻而复杂的冲突。

不当收集与利用的权利侵害：许多企业在“用户协议”的掩护下，未经用户充分知情和明确同意，过度收集个人信息，其范围远超提供服务所必需。这些数据被用于构建用户画像，进行精准营销、信息轰炸，甚至实施“大数据杀熟”等价格歧视行为。这种做法不仅导致用户隐私泄露和财产损失，更在精神层面造成用户的困扰与不安。

数据合并技术的隐私风险：大数据与云计算技术的发展，使得企业能够轻易整合来自线上线下、不同渠道的个人数据。例如，将用户的社交媒体活动、电商购物记录、线下消费习惯、地理位置轨迹等信息进行匹配与合并，构建出一个360度的全景式个人档案。这种技术极大地加剧了个人隐私的暴露风险，使得单一场景下的隐私保护措施形同虚设。

数据垄断对市场秩序的破坏：大型科技公司凭借其平台优势积累了海量用户数据，形成了强大的数据壁垒和市场垄断地位。它们利用数据优势精准打击竞争对手，限制创新，阻碍了市场的公平竞争。而部分中小型企业为了在竞争中生存，可能不惜采取非法手段，催生了庞大的数据窃取和买卖的黑色产业链。这不仅严重侵犯了个人信息权益，也破坏了健康、有序的市场竞争环境，最终损害消费者福祉。

2.2 公共安全与个人信息权益的冲突

公共安全作为社会的核心公共利益，其实现往往需要以对个人信息的收集与利用为前提，这就不可避免地与个人信息权益产生冲突。尤其是在反恐、打击犯罪、维护国家安全、应对突发公共卫生事件等领域，政府机构为了有效应对复杂的安全威胁，往往需要扩大信息收集的范围和权限。比如在突发公共卫生事件中，政府需收集公民的行程轨迹、健康状况等信息以阻断疫情传播，这类信息收集虽为公共安全所需，却也让公民的私人生活细节面临暴露风险。

例如，“9.11”事件后，美国出台的《爱国者法案》显著加强了政府在公共安全领域对个人信息的监控权力。近年来，各国政府纷纷利用人脸识别、大规模视频监控、网络通信监控等技术手段提升社会治理能力。这些措施在一定程度上提升了社会安全水平，但也引发了关于大规模监控是否侵犯公民隐私权的激烈辩论。如何在有效维护公共安全与保障个人隐私之间找到平衡，成为各国政府面临的共同挑战。这其中，“比例原则”是关键的考量标准：即为了公共安全对个人信息的限制，是否是必要的、适当的，并且其对个人权益的损害是否与所追求的公共利益相称[2]。缺乏透明的监督机制和权利救济渠道，可能导致公共权力被滥用，使公共安全成为侵犯个人隐私的借口。

2.3 社会公共利用与个人信息权益的冲突

大数据技术在医疗、交通、教育、科研等领域的公共利用，极大地提升了社会运行效率与公共服务水平，但在创造巨大公共价值的同时，也对个人隐私构成了潜在威胁，引发了深刻的伦理与法律冲突。

在医疗健康领域，利用海量的患者病历、医学影像、基因序列等高度敏感信息进行大数据分析，有助于疾病预测、药物研发和个性化治疗方案的制定。然而，这些信息的泄露或滥用，可能导致患者遭受歧视，甚至对其家庭成员产生影响[3]。如何在推动医学进步的同时，确保患者隐私和数据安全，是智慧医疗发展的核心难题。

在智能交通领域，通过收集车辆实时轨迹、公众出行习惯等数据，可以有效优化交通流量、规划公共交通线路、提升城市运行效率。但这些精细的地理位置数据同样是强隐私信息，长期、连续的轨迹数据足以揭示个人的生活模式、社交关系等私密信息，如何在提升便利性的同时避免个人行踪被过度追踪，是智能交通建设必须面对的挑战。

在教育、科研及舆情监控等其他公共应用场景中，同样离不开对个人信息的采集与分析。例如，教育决策可能依赖于学生的学业成绩、家庭背景等数据，但这可能加剧教育不公和算法歧视；社会科学研究需要大量样本数据，但如何确保数据在采集和使用过程中的匿名化和伦理合规性至关重要；而利用大数据进行舆情监控，虽有助于政府了解民意，但也存在模糊公共管理与侵犯个人言论自由、隐私权之间界限的风险。因此，如何在推动社会进步、实现公共利益最大化的过程中，划定个人信息利用的合理边界，是大数据时代必须解决的重大课题。

3 功利主义框架下的平衡策略

3.1 法律层面：构建趋利避害的制度框架

立法的利益平衡：立法过程本身就是一次功利主义的计算。它需要深刻权衡信息自由利用带来的巨大“快乐”与个人隐私被侵犯所导致的“痛苦”。一部良法，应力求在个人信息保护法中明确界定个人信息的范围、敏感度分级，以及信息主体的知情同意、查询、更正、删除等权利，更要引入“数据最小化”、“目的限制”、“存储期限限制”等核心原则。同时，法律必须审慎设定例外条款，其正当性基础应建立在比例原则之上，即任何对个人信息的限制都应当是为了实现合法的公共或第三方利益，且手段是必要、适当和相称的。穆勒的“伤害原则”为此提供了一个重要的伦理参照，强调了对个人自由干预的审慎性，但现代立法还需综合考虑更广泛的合法基础和多元的利益平衡。这些例外条款的适用条件和审批程序必须严格

限定，并建立相应的监督与问责机制，防止其成为权力滥用的后门，确保其总体效果是增进而非损害社会福祉。

信息流通的规则立法：面对信息数据不可逆转的产业化趋势，法律需要构建“在保护中利用，在利用中保护”的二元制度框架。这要求我们承认个人信息在特定场景下具有的财产属性，探索赋予信息主体对其数据财产的一定控制权、收益权和选择空间，例如通过数据信托、数据合作社等创新模式，让个人能更好地参与数据价值的分配。同时，依据信息的敏感程度和应用场景进行分类管理，对涉及公共利益或高风险的数据处理活动施加更严格的监管，确保信息在规范、安全的轨道上流通[4]。这一思路旨在激发数据要素的经济潜力，同时守住个人权益的底线，最终实现社会总效用的提升。

强化法律执行与监管：正如边沁所主张的，法律是实现社会功利最大化的关键工具，但徒法不足以自行。为了确保功利主义的计算在实践中得以落实，必须建立一个权威、独立、资源充足的数据保护机构。执法机构要加大执法力度，对违法行为采取零容忍态度，通过高额罚款、吊销许可、追究个人责任等严厉措施形成有效威慑。这些外部制裁，是引导行为符合社会规范的重要力量。此外，还应畅通个人权利救济渠道，支持公益诉讼，降低个人维权成本，让每个信息主体都能成为自身权益的积极守护者，从而形成一个能够动态调整、持续优化社会整体利益的治理格局。

3.2 社会层面：培育内在的道德自觉

强化隐私教育与数字素养：应将隐私保护和数据安全教育纳入国民基础教育体系，并利用多种渠道向公众普及相关知识。教育的目标不仅是让公众意识到风险，更是提升其“数字素养”，即培养公众辨别风险、管理隐私、行使自身合法权利的实践能力。这是在社会层面培育功利主义“良心”的基础，只有当公众普遍具备了基本的隐私保护意识和技能，才能从需求侧推动企业和机构更加重视数据安全，形成追求社会共同利益的文化氛围。

推动行业自律与责任共治：在政府强监管之外，行业的自我约束是培育组织“良心”的关键。应鼓励行业协会和龙头企业率先制定并执行高于法定标准的自律规范，推广“默认隐私保护”和“设计阶段隐私保护”的理念，将对他人福祉的关切内化为产品设计和业务流程的核心要素。通过建立行业内的隐私保护认证体系和最佳实践分享机制，引导整个市场向更负责任、更可持续的方向发展，使其行为不再仅仅受外部压力的驱动，而是源于内心的道德自觉[5]。

促进技术创新与法律融合：技术是挑战的来源，同样也是解决方案的关键。应大力鼓励和支持隐私增强技术的研发与应用，例如差分隐私、同态加密、联邦学习等。这些技术能够在不损害数据利用价值的前提下，最大程度地保护个人隐私。推动这些技术创新与法律规则的深度融合，通过“技术遵从”的方式，可以从源头上降低隐私泄露的风险。这正体现了功利主义的实践导向：利用一切可行的手段，寻求能够实现最大社会净收益的最优解。

4 结语

在功利主义的框架下，探讨个人数据利用与保护的平衡问题，其核心目标是在最大化社会整体福祉的同时，合理界定个人隐私权的边界与信息自由的空间。这意味着政策与法律的制定，本身就是一场持续的、动态的社会效益计算：既要有效保护个人隐私不受侵犯，以维护社会稳定与信任，又要促进信息的合理自由流通，以激发经济活力与社会创新。一个公正、高效的数据治理体系，需要政府、企业与公众的共同努力。政府应加强立法与监管，企业需履行社会责任，公众则要提升隐私保护意识。通过多方协同，我们才能共同构建一个既能保障个人权利又能释放数据价值的良性生态环境，最终在实践中不断趋近“最大多数人的最大幸福”这一理想目标。

参考文献：

[1] 威廉姆·H. 肖，庄忠正. 自由与功利主义——论约翰·穆勒的“自由原则”[J]. 学习与探索，2014,(02):37-42.

[2] 王长杰. 大数据侦查与个人隐私信息保护平衡问题研究[J]. 中国人民警察大学学报，2022,38(9):55-62.

[3] 田广兰，徐艳东. 生命功利主义：意大利Covid-19重症治疗的伦理原则[J]. 东南大学学报(哲学社会科学版)，2021,23(6):29-38.

[4] 杨琴，余计灵. 论数据库信息应用中如何协调个人信息保护与公共利益的平衡[J]. 法制与社会，2014(27):174-175.

[5] 沈琪章. 大数据功利主义计算逻辑中的"道德囚徒"[J]. 太原学院学报（社会科学版），2023,24(1):9-15.

作者简介：蒲世豪（1999.12—），男，四川广元市，硕士研究生，研究方向：法理学。