

反垄断法视角下电子商务数据隐私保护与消费者权益的平衡机制研究

李双双

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年5月8日; 录用日期: 2025年5月27日; 发布日期: 2025年6月30日

摘要

数字经济时代, 电子商务平台通过数据垄断与算法权力扩张, 导致消费者数据隐私侵害与市场结构失衡的叠加风险日益凸显。本文以《反垄断法》为研究视角, 聚焦电子商务场景下数据隐私保护与消费者权益的冲突本质及平衡路径。研究发现: 其一, 平台经济中“知情同意”规则的失效、数据要素市场化需求与隐私保护成本的矛盾、算法推荐引发的隐私泄露风险, 共同构成法理、经济与技术维度的多重冲突; 其二, 传统私法赋权与公法监管存在局限性, 难以矫正垄断性市场结构下的“数据权力”压迫, 亟需反垄断法通过市场势力规制介入数据隐私保护。基于对欧盟GDPR与美国CCPA的差异化路径分析, 结合中国《反垄断法》《个人信息保护法》协同实施需求, 提出“结构矫正-行为规制-技术协同”三位一体的平衡机制, 通过数据驱动型并购审查中的隐私竞争评估、滥用市场支配地位行为的分类规制(剥削性与排他性滥用), 结合联邦学习与区块链技术赋能隐私保护, 重构平台责任与消费者选择权保障体系。研究结论表明, 反垄断法可通过打破数据垄断格局、优化非价格竞争质量维度, 系统性提升电子商务场景下的隐私保护水平, 为数字经济治理提供兼具理论创新性与实践可行性的解决方案。

关键词

反垄断法, 电子商务, 数据隐私保护, 消费者权益, 平衡机制, 平台经济

Research on the Balancing Mechanism between E-Commerce Data Privacy Protection and Consumer Rights from the Perspective of Antitrust Law

Shuangshuang Li

Law School, Guizhou University, Guiyang Guizhou

Received: May 8th, 2025; accepted: May 27th, 2025; published: Jun. 30th, 2025

文章引用: 李双双. 反垄断法视角下电子商务数据隐私保护与消费者权益的平衡机制研究[J]. 电子商务评论, 2025, 14(6): 3309-3319. DOI: 10.12677/ec.2025.1462117

Abstract

In the era of the digital economy, the dual risks of consumer data privacy infringement and market structural imbalances caused by e-commerce platforms' data monopolies and algorithmic power expansion have become increasingly prominent. This study adopts the perspective of China's Anti-Monopoly Law to explore the inherent conflicts and equilibrium pathways between data privacy protection and consumer rights in e-commerce. Key findings reveal: 1) Multidimensional conflicts arise from the failure of the "informed consent" principle in platform economies, contradictions between data element marketization demands and privacy protection costs, and algorithm-driven privacy leakage risks, spanning legal, economic, and technological domains; 2) Traditional private law empowerment and public law regulation exhibit limitations in rectifying "data power" oppression under monopolistic market structures, necessitating antitrust intervention through market power regulation. By analyzing divergent regulatory approaches under the EU GDPR and U.S. CCPA, and addressing China's need for coordinated implementation of the *Anti-Monopoly Law* and *Personal Information Protection Law*, this research proposes a tripartite balance mechanism integrating "structural correction-behavioral regulation-technological synergy". Specific strategies include privacy competition assessments in data-driven merger reviews, categorized regulation of market dominance abuses (exploitative vs. exclusionary practices), and privacy protection empowerment through federated learning and blockchain technologies to reconstruct platform accountability and consumer choice safeguards. The conclusions demonstrate that antitrust law can systematically enhance e-commerce privacy protection by dismantling data monopolies, and optimizing non-price competition quality dimensions, thereby providing theoretically innovative and practically viable solutions for digital economy governance.

Keywords

Anti-Monopoly Law, E-Commerce, Data Privacy Protection, Consumer Rights, Equilibrium Mechanism, Platform Economy

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

2018 年, Facebook-Cambridge Analytica 数据门事件曝光¹。本案中, Cambridge Analytica 为帮助 2016 年特朗普竞选和英国脱欧等政治活动精准投放广告, 采取非法手段通过第三方应用接口获取 8700 万用户数据用以构建心理画像模型。这一行为直接暴露了平台在数据聚合中的三重风险: 其一为数据合规漏洞。Facebook 未有效审核第三方应用的数据使用目的, 违反 GDPR 的“目的限定原则”和“数据最小化原则”, 导致用户数据被用于政治商业用途而非声明的学术研究。其二为市场控制力对外延伸。通过社交图谱与行为数据的整合, Facebook 形成“超级用户画像”能力, 显著提升广告市场的进入壁垒。德国联邦卡特尔局在 2019 年裁决中指出, Facebook 为巩固其市场支配地位, 采用跨平台数据整合的方式合并 WhatsApp、Instagram 数据等做法构成剥削性滥用²。其三为法律协同治理需求。欧盟委员会在 DoubleClick 被谷歌收购案中确立的“两阶段分析法”在此事件中得到验证, 即先依据数据保护法判断数据收集合法性, 再评

¹Bundeskartellamt. Case KVR 69/19-Facebook, Decision of 15 August 2019.

²Federal Trade Commission. FTC v. Facebook, Inc., No. 1:19-cv-02180 (D.D.C. 2020).

估数据聚合对竞争的影响。然而，德国监管机构突破此框架，直接将隐私保护水平下降视为竞争法意义上的损害，推动隐私保护与反垄断规则的融合。该案件不仅是数据隐私保护的里程碑案例，更是数字平台通过数据整合形成跨领域市场控制力的典型体现。

无独有偶，阿里巴巴要求商家“二选一”的排他性协议也向竞争法提出了挑战。阿里巴巴利用交易数据、用户偏好等资源形成“数据-流量”闭环，迫使商家放弃多平台运营。根据中国市场监管总局 2021 年处罚决定，阿里巴巴通过算法监控商家跨平台行为，并对违规者实施搜索降权、流量限制等惩罚，实质是以数据控制能力排除竞争。而商家因退出成本过高被迫接受排他条款，形成“锁定效应”，造成纵向市场结构扭曲^[1]。此现象印证了杨祖卿提出的“数据隐私保护与竞争损害联动”理论——平台通过降低隐私保护水平(如扩大数据收集范围)换取竞争优势，同时挤压中小竞争者生存空间^[2]。

以上两起案例共同揭示了数据治理的核心问题，即数据要素流通效率与隐私保护、公平竞争如何达到平衡？正如欧盟竞争专员维斯塔格所言：“在数字时代，隐私保护不再是孤立的权利问题，而是市场公平竞争的前提”³。故本文认为数据聚合的违法性判定需突破部门法割裂，构建“数据保护法-反垄断法-技术标准”三维治理体系。未来立法应聚焦数据权力的制衡，防止平台通过数据垄断扭曲创新生态与民主进程。

2. 电子商务数据隐私与消费者权益的冲突本质

消费者隐私则是在隐私的基础上、从学理角度所提出的一种新概念，是为生活消费需要而购买、使用商品或者接受服务的自然人所享有的关于个人信息、私人活动及私有领域不被非法侵扰、收集、利用的人格权，消费者对于这些隐私事项是否公开以及公开的程度、范围、内容等享有自主决定权。在数字经济的浪潮中，消费者隐私权作为新型人格权，其保护与电子商务平台的数据利用需求形成了深刻的法理与实践冲突。这一矛盾的本质源于数据要素市场化需求与隐私人格权保护之间的结构性张力：一方面，平台经济依赖海量消费者数据优化服务、驱动创新，形成“免费换数据”的商业模式；另一方面，信息不对称、技术权力失衡及法律规制滞后，导致消费者对个人信息的控制权被系统性削弱。具体而言，冲突的显性化表现为以下三重维度：

2.1. 法理冲突：权利对抗与制度割裂

数据财产权与人格权的二元属性争议根植于现行法律体系的制度性断裂。《民法典》第 127 条将数据纳入民事权益范畴却未明确其权利属性，而《数据安全法》第 3 条将数据定位为“重要生产要素”，二者在价值取向上形成了结构性矛盾。这种立法割裂直接导致数据治理中人格权与财产权的法理冲突：一方面，《个人信息保护法》第 4 条基于“可识别性”标准强化对隐私权、知情权等具体人格权益的保护，要求数据处理需以“最小必要”为原则；另一方面，数据要素市场化改革要求释放数据流通价值，平台通过用户画像、行为模型等衍生数据的商业化利用创造经济收益。然而，法律未清晰界定人格利益与财产价值的边界，使得平台常以“数据加工”为由主张对衍生数据的排他性权利。例如，电商平台基于用户浏览记录生成的消费偏好模型，虽包含个人行为特征的人格属性，却被视为平台“劳动成果”而垄断使用。这种权利归属的模糊性不仅削弱个人对数据的控制权，更引发“保护-利用”的制度失衡。当平台援引《数据安全法》主张数据流通自由时，个人依据《个人信息保护法》要求撤回同意的权利往往被技术壁垒所架空，形成“法律赋权而技术剥夺”的实践悖论。

权利归属的模糊性进一步加剧人格权与财产权的张力，核心争议在于数据衍生价值的分配规则缺失。

³ 欧盟委员会新闻稿(2020 年 12 月 15 日)关于《数字市场法案》的说明中，维斯塔格强调“数据控制权的失衡将扭曲市场竞争，隐私保护是市场健康运行的必要条件。”

欧盟 GDPR 通过第 20 条“数据可携权”赋予用户跨平台迁移原始数据的权利,但我国法律尚未明确平台是否需开放数据接口,导致消费者难以实现数据自主。例如,社交平台积累的用户关系链数据虽源于个人社交行为,但平台以算法优化为由拒绝向第三方共享,实质将人格权益转化为商业壁垒。更深层矛盾体现在数据价值创造的认定逻辑上。个人作为数据源提供初始信息,平台通过算力与算法投入完成价值增值,二者对数据权益的贡献度缺乏量化标准。这种法理困境导致司法实践中出现“双重标准”。在微信读书隐私侵权案件中⁴,法院认定好友列表属于隐私范畴,强调个人对数据的控制权,而在反不正当竞争纠纷中则倾向保护平台数据权益,如“新浪微博诉脉脉案”⁵就认定平台对用户信息享有竞争性权益。要破解这一困局,需重构数据权利体系,在区分原始数据与衍生数据的基础上建立分级确权机制。因此,本文认为,原始数据因直接关联个人身份应强化人格权保护,衍生数据则依据加工投入赋予平台有限财产权,同时通过强制许可制度平衡公私利益。唯有厘清权利边界,才能实现数据要素市场化与人格尊严保障的协同发展。

2.2. 经济矛盾：市场激励与保护成本的对立

数据要素市场化需求与隐私保护成本的博弈,本质上揭示了数字经济中效率与公平的结构性矛盾。以“免费换数据”模式为核心的平台经济逻辑,将消费者隐私权益异化为数据生产要素的廉价来源,形成制度性剥削关系。社交平台常见做法是通过零价服务吸引用户,却在用户协议中嵌入数据采集条款,利用算法将私人活动信息转化为可交易的定向广告资源。这种模式下,平台凭借数据规模化收集实现边际收益递增,而隐私保护成本,如加密技术投入、合规审计等,却通过“知情同意”的形式化机制转嫁给消费者。美国《加利福尼亚州消费者隐私保护法》(CCPA)的“选择退出”机制即暴露此矛盾:企业默认享有数据收集权,用户需主动行使权利才能退出,但复杂的操作流程与技术壁垒使得实质退出率不足 3% [3],隐私保护成本实质上由消费者承担。更深层问题在于数据定价机制的缺失。当前数据价值评估体系尚未建立,消费者无法通过市场交易实现数据收益分成。在上述案例中,Facebook 定向广告收入占总营收 98%,但用户既无法量化自身数据贡献,亦无法获得经济补偿,形成“数据贡献-商业收益”的单向流动[4]。这种失衡源于数据权属的模糊性:平台以“数据加工”为由主张衍生数据所有权,而消费者对原始数据的控制权被《数据安全法》的生产要素定位所稀释。欧盟《数字市场法案》(DMA)试图破解此困局,要求“看门人”平台开放数据接口并禁止自我优待,但实践中仍面临数据分类确权与利益分配的技术难题。

垄断性市场结构则通过技术权力与制度惯性进一步剥夺消费者选择权,加剧隐私权益的不可逆流失。网络效应与用户锁定效应构筑的“数字牢笼”,使得消费者即便意识到隐私侵害,也难以承担迁移成本。用户因社交关系链与使用习惯被绑定,即使新平台提供更严格的隐私保护,重新建立社交图谱与数据授权的成本仍远超个体承受阈值。平台更通过行为设计强化“自愿性压迫”:亚马逊 Prime 会员以“一键续费”和定向折扣诱导用户放弃数据控制权,算法推荐系统则利用认知偏差制造“信息茧房”,使消费者在无意识中持续授权数据采集。这种选择权的系统性虚置,本质是垄断权力对市场机制的扭曲。当平台凭借数据垄断形成市场支配地位滥用,消费者即便行使《个人信息保护法》规定的删除权,亦可能因数据再生能力(如通过关联数据重建用户画像)而陷入“删除-再生-再删除”的无限循环(杨祖卿, 2023) [2]。反垄断法的介入需突破传统分析框架:在 Meta/Within 并购案中⁶,FTC 首次将“隐私保护竞争削弱”纳入审查标准,指出 VR 健身数据垄断可能降低行业隐私创新动力。这提示未来规制需从结构矫正转向行

⁴北京互联网法院(2019)京 0491 民初 16142 号民事判决。

⁵北京知识产权法院民事判决书(2016)京 73 民终 588 号[Z]。2016。

⁶<https://mp.weixin.qq.com/s/h0Xo3Q7WliaNcdVYxBKsXw>。

为 - 效果综合评估, 通过强制数据可携、打破算法黑箱等工具, 重构消费者与平台的力量平衡, 使隐私保护真正成为市场竞争的差异化维度而非垄断者的牺牲品。

2.3. 技术张力：算法权力与隐私风险的失控

精准推荐算法与隐私泄露的关联性本质在于用户画像技术的合规边界模糊化, 其通过跨场景数据融合与算法黑箱化突破隐私保护底线。平台利用购物记录、地理位置、社交关系等多维度数据构建用户画像时, 常通过过度关联分析推断出敏感信息。美国 Target 公司通过分析用户购买无味湿巾与营养补充剂等商品, 精准预测女性妊娠状态并定向推送母婴产品广告, 这一案例揭示了数据聚合如何从非敏感行为中提取高度私密信息[5]。此类分析不仅违反《个人信息保护法》中的“最小必要”原则, 更因数据使用目的的不可预见性架空用户知情权。更深层风险在于算法的不可解释性: 深度学习模型的“黑箱”特性使数据处理逻辑对用户完全封闭。以生成式人工智能(AIGC)为例, 其可能通过隐蔽模块实时采集用户交互数据, 用于训练迭代或商业挖掘, 但用户既无法追溯数据流向, 也难以通过现有法律主张删除权。这种技术特性与法律规制的错位, 导致平台在“提升服务精准度”的名义下, 将隐私侵犯隐匿于算法复杂性之中。欧盟《数字服务法案》(DSA)虽要求平台公开推荐算法的主要参数, 但实践中仅披露泛化的数据处理目的(如“优化用户体验”), 未能解决用户对数据二次利用及跨平台共享的实质性质疑。当技术能力远超法律解释框架时, 消费者往往陷入“知情却无力控制”的被动局面, 隐私保护沦为形式合规而非实质保障。

数据匿名化技术的局限性则暴露于重识别风险与动态技术迭代的双重夹击下, 传统去标识化方法在大数据环境中逐渐失效。匿名化数据可通过跨数据集关联还原个体身份, 如 2006 年 AOL 公布 2000 万条匿名搜索记录后, 研究者通过“咖啡店”“乳腺癌”等关键词关联公开的选民登记信息, 成功锁定真实用户。此类风险源于数据要素的强关联性, 医疗数据中的罕见病记录、位置轨迹中的高频停留点等, 均可成为破解匿名化的“密钥”。尽管差分隐私技术通过添加噪声降低重识别概率, 但其数据效用损耗与隐私预算的平衡难题制约了商业应用。联邦学习虽实现“数据不动模型动”, 但模型参数仍可能泄露成员信息, 如通过反演攻击从共享梯度中推断用户原始数据。更严峻的挑战来自技术迭代的不确定性, 量子计算的发展可能突破现有加密算法的防护阈值, 使得当前符合 ISO/IEC 27701 标准的数据匿名化措施在未来丧失安全性。企业因此陷入合规悖论——既要承担高昂的动态技术升级成本(如每两年更换加密协议), 又需应对法律对“充分匿名化”的静态认定标准。欧盟 GDPR 第 25 条要求的“通过设计与默认的数据保护”原则, 在实践中因技术滞后性难以落实, 医疗、金融等领域被迫在数据开放价值与隐私风险间艰难取舍。当匿名化从技术问题演变为系统性风险时, 单一技术改良已无法应对, 需构建包含数据生命周期管理、跨域协作治理及弹性法律框架的复合型防护体系。

电子商务数据隐私与消费者权益的冲突本质, 体现了数字时代“权利 - 经济 - 技术”三重维度的结构性矛盾。法理冲突源于数据权力与个人权利的对抗, 经济矛盾反映市场激励与保护成本的失衡, 技术张力则暴露算法霸权对隐私的侵蚀。解决路径需突破单一法律框架, 构建公私法协同、市场激励与技术治理融合的新型规制体系。欧盟《数字市场法》强制平台开放数据接口, 我国《个人信息保护法》引入“数据可携带权”试点, 均指向通过结构性改革破解“垄断 - 隐私”恶性循环。未来研究需进一步探索技术标准与法律规则的兼容性, 以实现数据价值释放与隐私保护的双重目标。

3. 反垄断法介入平衡机制的理论及法律基础

3.1. 理论依据：从市场失灵到制度矫正

在数字经济生态中, 数据隐私保护与商业利益的冲突源于市场机制无法自发实现社会总效用的最优

配置,这种结构性失衡导致市场自我调节机制失效,典型表现为平台通过交叉数据画像提升商业价值的同时,用户对隐私泄露风险的控制权却持续弱化。

在数据隐私保护的语境下,卡尔多-希克斯改进需结合平台经济的网络效应特征,构建“社会福利净现值(NPV)模型”。例如,德国联邦卡特尔局在 Facebook 案⁷中通过隐私感知指数(PSI)量化用户隐私效用损失,并将其与广告效率提升带来的经济效益进行动态平衡。若数据聚合的社会福利增量(如广告精准度提升)超过隐私损害(如用户焦虑值增加),则符合卡尔多-希克斯效率改进的基本逻辑;反之则需通过反垄断罚款强制建立专项补偿基金。卡尔多-希克斯效率模型通过法律强制实现社会福利的帕累托改进,也即即便存在部分利益受损者,只要社会总体收益能够覆盖补偿成本即可达成动态均衡。该效率模型在数字经济中的应用需突破传统补偿逻辑,结合数据要素的动态性与网络效应特征,构建“收益-损失-补偿”的三维评估框架。具体可从以下维度展开:

一是对社会福利增量测算。数据聚合的经济效益需通过“边际收益递减曲线”与“网络效应乘数”综合评估。德国联邦卡特尔局对 Facebook 跨平台数据整合的测算显示,广告点击率提升的同时,通过隐私感知指数 PSI 测量用户隐私概率却在增加,在此引入“社会福利净现值(NPV)”模型可判定数据垄断的合理性。

二是创新抑制的实证验证。通过赫芬达尔指数(HHI)与研发投入比的关联性分析可量化市场集中度对创新的影响。平台通过跨场景数据整合提升广告点击率,需量化其对消费者剩余及创新抑制的综合影响。当数据垄断导致隐私保护水平下降时,可通过反垄断罚款建立专项补偿基金,或要求平台提供差异化服务选项以实现帕累托改进。

三是专项补偿基金的法律化运行。美国 FTC 对 Facebook 的 50 亿美元罚款转为隐私技术研发基金,需建立“收益-补偿”闭环机制,如强制平台将数据垄断收益的 5%~10%注入基金池,并通过第三方独立审计确保资金流向透明。

反垄断执法介入隐私保护领域时,比例原则成为平衡多方利益的核心准则。比例原则需从“静态审查”转向“动态适配”,结合数据生命周期与市场竞争结构分层实施:

一是在必要性层面禁止超范围数据采集。必要性层面要求数据收集范围与商业目标严格匹配,中国《个人信息保护法》第 6 条确立的“最小必要原则”在司法实践中展现出其具有约束力。甘肃银行因强制读取用户短信记录被罚 120 万元,法院认定信贷风险评估无需获取通讯内容,过度采集构成侵权⁸。除甘肃银行案外,瑞典隐私保护局对金融公司 Klarna 的处罚也进一步明确,数据收集范围需与场景风险等级匹配,如信贷评估仅需验证还款能力,禁止采集社交关系链等非必要信息。同时,也需要进行合规验证。通过对数据进行标签化并纳入系统,从而对数据类型(如生物特征、位置轨迹)进行敏感度分级、区块链存证,实现全流程可追溯。

二是在适当性层面通过结构性救济分离高敏感数据库。适当性标准强调隐私保护强度与市场竞争需求适配,欧盟在审查 Google 收购 DoubleClick 案时⁹,虽认可数据整合带来的广告效率提升,但为防止搜索数据与广告数据融合形成市场壁垒,强制要求谷歌承诺十年内不合并两类数据库,这种结构性救济既维护了数据流动效率又遏制了垄断风险。从此案中可学习强制分离数据库的做法,通过“数据沙盒”机制优化,允许平台在隔离环境中测试数据聚合效果并设试验期,根据市场集中度变化动态调整限制期限。同时,设置技术中立的监管模式。通过机器学习模型预测市场恢复周期,初犯处罚力度与恢复周期

⁷Wiedemann, K. (2020). A Matter of Choice: The German Federal Supreme Court's Interim Decision in the Abuse-of-Dominance Proceedings Bundeskartellamt v. Facebook (Case KVR 69/19). IIC-International Review of Intellectual Property and Competition Law, 51, 1168-1181.

⁸<https://mp.weixin.qq.com/s/aNxYiCFrVzo17bxZF9x3ww>.

⁹Trotta, Christina T. 2007. "The Google-DoubleClick Merger, the FTC, and the Future of Transactional Privacy Inquiries in the United States." SSRN.

负相关。

其三在狭义比例性层面动态调整罚款比例，可设置“成本－收益”的动态均衡模型，具体体现在执法成本与公共利益保护的动态平衡。在 Facebook 数据案中¹⁰，美国 FTC 对 Facebook 的 50 亿美元罚款虽创历史纪录，但仅占其年营收的 9%，相较于该平台通过违规数据利用获得的百亿美元级收益，处罚力度仍显不足。这种权衡折射出监管机构在维护市场秩序与保持创新活力间的复杂博弈，德国反垄断局在亚马逊数据滥用案中采用的初犯警告、累犯重罚的“阶梯式处罚”机制或是更优解，既形成威慑又不扼杀技术迭代空间。通过三阶比例原则的精细化应用，反垄断执法得以在数据价值释放与隐私权益保护之间构筑动态平衡。

3.2. 法律框架：公私法协同规制的路径

在数字经济快速发展的背景下，数据隐私保护与反垄断法的协同规制已成为破解市场失灵的关键路径。《反垄断法》第 22 条关于禁止“附加不合理交易条件”的规定，通过司法实践中的扩展解释，逐渐被赋予隐私审查功能。平台企业利用市场支配地位强制用户接受隐私条款的行为，本质上构成了对消费者选择权的系统性剥夺。市场监管总局在阿里巴巴“二选一”案中首次确认¹¹，平台要求商家共享用户数据作为流量支持的前提条件，不仅扭曲了市场竞争秩序，更通过数据控制权的集中化加剧了用户隐私风险。2023 年，德国联邦卡特尔局对 Meta 的执法实践进一步深化了这一逻辑。当平台隐私保护水平低于市场竞争标准，即便未直接限制同业竞争，也可被认定为“不合理交易条件”。这种解释范式突破了传统反垄断分析对价格因素的单一依赖，将隐私保护视为质量竞争的核心维度。侯晨亮、杨东(2022)的研究表明，头部平台通过数据条款捆绑形成的用户锁定效应，使消费者在隐私权让渡与服务质量获取之间丧失议价能力，导致市场自我调节机制失效[6]。为此，司法审查需建立“双轨评估标准”，即既要考察隐私条款是否实质性削弱用户控制权，如默认开启生物识别数据收集，也要验证平台是否通过数据垄断获取超额收益，如定向广告收入增幅与隐私条款严苛度正相关。这种动态平衡机制既维护了数据要素的市场流动性，又通过反垄断干预迫使企业将隐私保护成本内部化。

公私法协同规制的实现需要构建跨部门、跨领域的制度衔接机制。当平台行为同时违反《反垄断法》与《个人信息保护法》时，责任竞合问题的处理考验着法律体系的协同效能。例如金融 APP 过度收集用户轨迹数据的行为，既构成《个保法》第 66 条规定的违法处理个人信息，也可能因排除隐私保护创新竞争而触犯《反垄断法》第 22 条。对此可借鉴欧盟“一站式执法”机制，由反垄断机构与网信部门组建联合调查组，在证据采集、损害评估等环节实现信息共享与程序衔接。规则协同方面，《电子商务法》第 23 条可引入数据可携权制度，要求平台开放标准化数据接口。谢修涵(2023)的实证研究显示，数据迁移义务的设立能使新进入者通过差异化隐私政策获得 20%~35% 的用户转化率，有效打破既有平台的“数据孤岛”[7]。这种制度设计需平衡多方利益，对超级平台设置 6 个月过渡期以适应技术适配，对中小企业豁免接口开发义务以避免合规成本过载。同时，隐私计算技术的应用为协同规制提供了技术支撑。2023 年，中国信通院数据表明，联邦学习框架下多方安全计算能使数据使用效率提升 40%、隐私泄露风险降低 90%。但也需警惕技术中立性陷阱，美团外卖算法案揭示，即便采用差分隐私技术，若数据聚合量级超过临界点，仍可能通过逆向工程识别特定用户。这就要求法律与技术标准需联动更新，因此将隐私影响评估(PIA)纳入反垄断审查必备程序，确立“数据规模－脱敏强度－竞争效应”的三维审查模型，确保

¹⁰Business-Essay. n.d. “The Facebook-Cambridge Analytica Data Breach: A Case Study.”
<https://business-essay.com/the-facebook-cambridge-analytica-data-breach-a-case-study/>.

¹¹新华每日电讯。“市场监管总局依法对阿里巴巴集团控股有限公司在中国境内网络零售平台服务市场实施‘二选一’垄断行为作出行政处罚”。2021 年 4 月 11 日，http://www.xinhuanet.com/mrdx/2021-04/11/c_139872360.htm.

规制手段与数字市场复杂性相匹配是非常有必要的。

3.3. 技术赋能：隐私保护的技术实现路径

在数字经济治理中，隐私计算技术的突破为平衡数据价值释放与隐私保护提供了技术解方。联邦学习通过分布式机器学习框架，使得跨机构数据协作无需共享原始数据即可完成联合建模。以金融信贷风控为例，商业银行与电商平台在联邦学习框架下，各自持有的用户消费数据与征信数据通过加密参数交互实现风险评估模型训练，既保证了电商平台的交易数据不出库，又使银行获得更精准的授信决策依据[8]。这种“数据可用不可见”机制有效化解了《个人信息保护法》第13条规定的的数据最小化原则与商业数据融合需求之间的张力。多方安全计算技术则在医疗健康领域展现出独特价值，当疾控中心需联合多家医院进行流行病学分析时，通过秘密分享、同态加密等密码学协议，可在不暴露患者身份信息与诊疗细节的前提下，完成跨机构数据统计分析，使敏感医疗数据的科研价值得以释放而隐私风险可控。技术中立性风险亦需警惕，如联邦学习模型参数可能通过逆向工程反推原始数据特征，这要求法律规范与技术标准协同迭代，明确模型训练中的隐私预算阈值与数据脱敏强度，建立“技术实施-合规审计-责任追溯”的全流程治理框架。

区块链技术的分布式账本特性为数据治理提供了透明化追溯工具。在数据确权环节，智能合约可自动记录用户授权范围、使用场景及时效性，欧盟GDPR要求的“明确且具体的同意”藉此转化为可验证的链上存证。在支付宝开发的“蚂蚁链”实践中，用户每项数据授权均生成时间戳标记的哈希值，监管部门可通过节点权限实时调阅授权日志，使传统隐私保护中“告知-同意”原则的抽象要求转化为可验证的技术事实[9]。当发生数据泄露事件时，区块链的不可篡改特性可快速锁定泄露环节，如物流企业用户信息泄露案件中¹²，通过追溯数据访问链发现某第三方API接口未按规定进行访问权限隔离，技术存证为反垄断执法中的过错认定提供客观依据。技术赋能亦需与制度创新相协同，OECD在2021年数字经济治理报告中建议，数据驱动型并购审查可要求合并方部署区块链监管节点，确保并购后数据融合过程符合隐私保护承诺，这种“技术合规嵌入”机制既维持了企业技术迭代空间，又通过可验证的技术约束降低监管成本。隐私计算与区块链的协同应用，实质上是将卡尔多-希克斯效率改进模型中的社会福利计算转化为可执行的技术协议，使数据利用的正外部性与隐私保护的负外部性在算法层面实现动态均衡。

4. 制度优化与政策建议

4.1. 立法完善：从分散到体系化

1) 构建多维非经济性损害评估体系

反垄断法对隐私损失的量化评估需突破传统经济补偿框架，构建数据控制权受限与市场选择空间压缩的双维度分析体系。欧盟《数字市场法》(DMA)创设的“服务质量折损”评估机制具有方法论参考价值，具体可从三个技术路径展开：

一是数据控制权弱化的量化路径。通过用户行为追踪技术构建动态评估模型，系统记录用户对跨平台数据流动的知情撤回频率，并结合眼动追踪实验验证界面设计对用户数据权限认知的干扰效应。二是市场选择压缩的博弈论测算。基于修正型赫芬达尔指数(MHHI)构建数字市场结构模型，当头部平台占据市场份额超过一定阈值时，用户切换成本每增加相应比例，其接受不利隐私条款的概率则会提升。三是平台信任资本的价值折算。运用多模态情感分析技术处理非结构化数据，通过BERT模型解析社交媒体中隐私相关语义强度。当平台隐私事件引发的负面情绪占比超过基准值一定个百分点时，其用户月活留

¹²http://mp.weixin.qq.com/s?__biz=MjM5NzUyNTYwMw==&mid=2247552169&idx=3&sn=d6a655b53aead8a601db78616f2447d6&scene=0.

存率将出现滑坡情况。

2) 实施消费者权益导向的数据分级规制

现行《数据安全法》第 21 条的分类框架需向消费者隐私保护维度延伸, 构建“敏感数据禁止推定”原则。具体而言: 第一层级为生物特征、医疗记录等敏感数据, 适用 GDPR 第 9 条“必要性测试”标准, 要求平台证明数据收集与核心服务功能直接相关(如支付宝人脸识别需通过央行《金融 APP 必要个人信息范围》审查); 第二层级为浏览记录、位置轨迹等一般行为数据, 采用 CCPA “选择退出”机制, 强制平台在用户首次授权后每 90 天重新授权, 且撤回通道响应时间不得超过 24 小时; 第三层级为信用评分、消费画像等衍生数据, 依据法国竞争管理局对 Facebook 案的裁决, 要求平台在用户协议中明确数据共享范围, 禁止通过“数据池”条款独占使用权, 违者将按《反垄断法》第 22 条处上一年度销售额 5% 罚款。在具体实施路径上, 建议由国家网信办联合市场监管总局发布《数据分类分级操作指引》, 建立“数据标签-处理场景-合规义务”三维矩阵, 要求超级平台每季度提交数据流转图谱, 对未标注敏感数据类型的违规行为实施首次警告、二次限流、三次暂停数据业务“阶梯式处罚”。

4.2. 监管创新：从被动到主动治理

1) 构建“监管沙盒”机制：隐私保护与竞争激励兼容试点

监管沙盒机制通过划定安全试验空间, 推动隐私技术创新与市场活力的动态平衡[10]。在准入机制上, 企业需提交基于《ISO/IEC 29134》标准的隐私影响评估(PIA)报告, 重点验证联邦学习、多方安全计算等技术方案是否实现“数据可用不可见”的核心目标。例如, 新加坡金融管理局(MAS)在跨境支付沙盒中允许企业暂缓执行数据本地化要求, 通过加密传输与分布式账本技术测试跨境数据流动的合规性退出机制则需引入第三方独立评估机构, 对试点期满项目的隐私保护水平(如差分隐私预算控制)和市场竞争效果(如市场集中度变化)进行量化评分, 达标者可申请技术规模化应用。实践中, 蚂蚁集团在浙江试点的“隐私计算开放平台”通过沙盒机制验证了多方安全计算技术在信贷风控中的可行性, 既避免了数据垄断风险, 又使中小金融机构联合建模效率提升 40%。

2) 推行第三方合规审计：隐私保护水平认证体系

第三方审计体系以《ISO/IEC 27701 隐私信息管理体系》为核心框架, 重点核查数据收集的最小必要性(如是否超范围采集生物特征)和匿名化技术有效性(如 k-匿名化参数是否达到行业标准)。动态评级机制可参考声网隐私保护实践, 按平台规模与数据类型划分年度隐私保护指数(PPI), 其中 D 级平台需接受反垄断调查并暂停数据跨境业务。在激励措施方面, 高级别企业可享受税收减免及数据跨境流动便利, 欧盟-美国数据隐私框架(DPF)的“充分性认定”快速通道即为范例, 通过认证的企业可豁免数据传输个案审批。在法律衔接上, 修订后的《反不正当竞争法》要求平台首页公示审计结果, 未通过 ISO 27701 认证者不得参与政府采购或行业标准制定, 如某非银行支付机构因隐私政策不透明被处罚并限制市场准入。这一体系通过“认证-激励-惩戒”闭环, 倒逼企业将隐私合规内化为核心竞争力。

4.3. 平台责任：从合规到伦理设计

平台需构建全生命周期的隐私影响评估(PIA)体系, 将隐私风险管理贯穿产品研发、运营及迭代全流程。在事前评估阶段, 通过数据流转路径模拟, 如腾讯“数据护照”项目要求开发者提交数据使用场景图识别生物特征数据跨平台共享等潜在风险, 并开展压力测试验证隐私保护方案的可靠性; 事中监控阶段依托区块链技术实现数据调用记录的不可篡改存证, 确保监管部门可实时核查数据访问的合法性与必要性; 事后整改阶段引入“熔断机制”, 对触发隐私泄露阈值, 如对用户画像准确率与隐私暴露风险的正相关性超过预设值的算法进行强制暂停服务, 并参照欧盟《数字市场法》要求违规平台在 48 小时内提

交整改方案。同时，平台需建立双向透明度机制，监管侧需强制提交算法逻辑说明书，详细披露数据处理目的、特征变量权重及决策阈值并接受第三方技术审计以符合《个人信息保护法》第 24 条要求；用户侧需提供可解释性交互界面，如个性化推荐页面增设“一键反推”功能，展示推送内容的关键数据维度，允许用户通过滑动条自主调节隐私保护等级。此外，应设立算法伦理审查委员会，对涉及医疗健康数据定价等敏感场景的算法进行公平性评估，防范数据偏见导致的系统性歧视，实现技术合规与伦理设计的双重约束。

4.4. 消费者赋能：从弱势到主动参与

1) 数字素养教育计划：构建全场景隐私能力培育体系

针对数字时代消费者隐私保护能力不足的痛点，需建立“政府-企业-社会组织”协同教育体系。在基础教育层面，在中小学课程嵌入“数据权利”模块，通过欧盟“数字公民计划”式案例教学，培养学生解析隐私政策关键条款的能力，如识别生物特征数据二次利用风险。在定向培训领域，面向老年人、低收入群体开展社区工作坊，参考韩国 KISA“银发数字护航”项目设计适老化交互界面，手把手指导关闭非必要权限、识别钓鱼链接等实操技能。在技术赋能方面，开发类似德国消费者协会“数据足迹追踪器”的“隐私计算器”APP，运用联邦学习技术实现本地化风险评估，实时预警高风险行为。在政策配套上，将隐私素养指标纳入《全民科学素质行动纲要》，对完成培训者颁发“数字公民安全认证”，该认证可作为求职、信贷场景的信用加分项，同时对企业参与培训项目给予税收减免激励，形成隐私能力建设的正反馈机制。

2) 公益诉讼制度革新：突破集体救济的司法瓶颈

为破解消费者个体维权成本高、举证难的困境，需系统性重构公益诉讼制度。在诉讼主体方面，借鉴巴西《消费者保护法》第 82 条，赋予消费者协会代表不特定多数用户提起反垄断公益诉讼的资格，如在平台强制收集地理位置数据案件中行使集体诉权。证据规则上引入“初步证据规则”，当企业明显违反《个人信息保护法》第 13 条的最小必要原则(如超范围采集通讯录信息)，由平台自证其数据行为未造成实质性损害。赔偿金分配机制参考美国 Facebook 数据门事件和解方案，将胜诉赔偿的 30%注入“隐私保护基金”，专项用于资助差分隐私算法研发及受害者救济，剩余部分支持第三方机构开展合规审计。在配套法律修订中，建议在《民事诉讼法》增设“数据隐私集体诉讼”专章，明确惩罚性赔偿按企业上年度营收 1%~5%动态计算，并参照欧盟《数字市场法》对系统性侵权实施顶格处罚，形成司法震慑效应。

本章提出的制度优化路径，以“立法重构-监管升级-技术赋能-公众参与”为逻辑主线，既回应了数字市场结构性失衡的深层矛盾，也为破解“隐私保护与商业利益”的零和困境提供了中国方案。未来需通过试点验证与动态调整，推动政策工具从理论设计向实践落地转化。

5. 结论与展望

本文聚焦数字经济时代电子商务平台数据隐私保护与消费者权益的冲突本质，揭示市场结构失衡是隐私保护失效的核心症结。平台通过数据垄断与算法霸权形成“数据-流量”闭环，导致消费者知情同意规则失效、数据要素市场化需求与隐私保护成本矛盾加剧、算法推荐引发隐私泄露风险三重结构性冲突。研究表明，传统私法赋权与公法监管因制度割裂与执行偏差难以矫正市场失灵，而反垄断法通过卡尔多-希克斯效率改进模型与比例原则的应用，能够系统性重构数据价值链。例如，欧盟《数字市场法》强制“守门人”平台开放数据接口，德国联邦卡特尔局对 Facebook 数据整合行为的剥削性滥用认定，均验证了反垄断法在平衡隐私保护与商业利益中的制度优势。技术赋能层面，联邦学习与区块链技术通过“数据可用不可见”与透明化追溯机制，为隐私保护提供了可落地的技术解决方案，但需警惕算法黑箱与匿名化技术局限性带来的新型风险。

但由于现有参考资料以及思维局限,未来研究仍需在以下方向深化探索:其一,元宇宙场景下的隐私挑战亟待回应,虚拟身份与生物识别数据的聚合可能加剧“深度画像”对人格权的侵蚀,需重新界定反垄断法在虚拟经济中的适用边界;其二,生成式人工智能(AIGC)的崛起带来监管空白,算法可解释性与数据再生能力的冲突需构建“技术伦理-竞争公平”协同治理框架;其三,跨国数据流动与执法协同问题尚未解决,如何协调 GDPR 与 CCPA 等差异化制度、应对量子计算对加密技术的冲击,仍需跨学科研究支撑。此外,实证数据的动态追踪与案例库建设将成为提升规制精准度的关键。本文为平台经济反垄断指南修订与数据要素市场化改革提供了理论依据,但需在制度弹性与技术迭代中持续完善,以实现数字经济高质量发展与消费者权益保障的长期均衡。

参考文献

- [1] 国家市场监督管理总局. 市场监管总局发布阿里巴巴集团控股有限公司在中国境内网络零售平台服务市场垄断案行政处罚决定书和行政指导书[EB/OL]. https://www.samr.gov.cn/zt/qhfdzf/art/2021/art_74b2593fd32a432baf3dcbd163935167.html, 2021-04-10.
- [2] 杨祖卿. 数字市场中的数据隐私保护: 维度拓展、实践困境及路径突破——基于反垄断法视角[J]. 南方金融, 2023(1): 65-77.
- [3] 安全内参|决策者的网络安全知识库. 美加州消费者隐私法案(CCPA)修正案汇总全文翻译(附下载) [EB/OL]. <https://www.secrss.com/articles/14479>, 2019-10-22.
- [4] 周汉华. 平行还是交叉个人信息保护与隐私权的关系[J]. 中外法学, 2021, 33(5): 1167-1187.
- [5] 丁晓东. 论算法的法律规制[J]. 中国社会科学, 2020(12): 138-159.
- [6] 侯晨亮, 杨东. 平台剥削用户数据的形态、成因及规制[J]. 中国特色社会主义研究, 2022(5): 76-83.
- [7] 谢修涵. 消费者数据隐私保护的反垄断法规制[D]: [硕士学位论文]. 合肥: 安徽大学, 2023.
- [8] 范一飞. 劳动者过度劳动法律规制分析[J]. 黑龙江人力资源和社会保障, 2021(15): 67-69.
- [9] 白硕, 范玲瑜. 数字经济背景下商业平台数据权属法律保护[J]. 商业文化, 2021(34): 10-11.
- [10] 邓建鹏, 李雪宁. 监管沙盒的国际实践及其启示[J]. 陕西师范大学学报(哲学社会科学版), 2019, 48(5): 62-76.