电商平台中个人信息保护的研究

潘煜萌

北方民族大学，宁夏银川，750021；

摘要：随着电商市场规模扩大，用户个人信息保护问题凸显。我国《个人信息保护法》推动电商平台从被动合规转向主动防护，但仍面临复杂挑战。实证研究发现，电商领域存在隐私协议形式化、定位跟踪技术滥用、算法歧视等问题，反映出技术伦理困境及制度治理缺陷。

探究成因，主要存在法律制度设计滞后、行政监管效能不足、行业自律机制不健全等结构性矛盾。为解决这些问题，需构建协同治理体系：一是完善法律制度，通过场景化立法规范技术应用边界，构建法律与技术双重治理模式，强化预防和救济闭环保护；二是强化行政监管，设立独立监管机构，提升国家标准强制力，建立精细化处罚机制，畅通监管渠道；三是健全行业自律体系，公开规则制定程序，建立多层次监督执行机制与多元化纠纷解决渠道，构建外部监督机构、通过法律规制、行政监管与行业自律三维协同，平衡用户信息权益保护与数字经济创新发展，为相关权利实现提供制度保障，构建兼顾个人权益保护与产业可持续发展的治理格局。

关键词：个人信息保护；电子商务平台；隐私权；个人信息自决

DOI：10.69979/3041-0673.25.08.065

1 电商平台中个人信息保护的实践困境

1.1 数据收集前：隐私协议的形式化困境

隐私协议作为用户授权的核心载体，存在显著的“文本异化”问题。

第一，可读性与获取障碍，超 90%用户因条款冗长（平均 1.5 万字以上）、术语晦涩（如“去标识化”、“差分隐私”缺乏量化标准）而放弃阅读，83.89%用户反对默认勾选“同意”选项。部分平台隐私政策入口隐蔽（如拼多多需 3 级菜单跳转），“显著告知”沦为“隐蔽告知”，用户被迫接受“要么同意、要么退出”的霸王条款。

第二，收集范围模糊与责任转嫁，尽管《个人信息保护法》要求“最小必要”原则，平台仍过度采集非必要信息（如淘宝收集麦克风权限用于“语音描述优化”却未提供关闭选项），并通过“概括授权”将数据共享给关联方（如阿里系平台内部无限制共享用户行为数据），但未列明第三方名称及用途，导致用户维权时责任主体不明。

第三，信息可携带权落地难，仅少数头部平台在隐私政策中提及可携带权，且数据导出范围有限（仅基础身份信息，不含行为分析数据）、格式不兼容（缺乏标准化接口），技术操作成本高，用户难以实际行使跨平台数据迁移权利。

1.2 数据收集中：定位与跟踪技术的滥用风险

技术应用的“便利化”与“失控化”并存，催生隐私边界侵蚀问题。

第一，定位技术过度采集，平台以“优化服务”为由持续收集地理位置信息，如美团根据用户位置动态调整商品价格、拼多多通过通讯录构建社交关系链。但位置信息作为敏感数据，一旦泄露可能导致精准诈骗、人身安全威胁，且平台对“必要采集范围”缺乏清晰界定，用户难以感知数据使用边界。

第二，跨平台跟踪技术的隐蔽性，Cookies、设备指纹、跨设备追踪（Cross-Device Tracking）等技术实现用户行为全场景记录，甚至监测其他应用活动。例如，淘宝通过设备标识符关联多端数据生成精准画像，用于高强度广告推送。用户对跟踪技术的感知度低，且“请勿跟踪”协议因缺乏法律强制力沦为摆设——超 70%第三方数据公司无视用户设置，继续共享行为数据。

第三，技术滥用的安全隐患，内部人员泄露（如物流行业“内鬼”）与非法技术攻击成为数据泄露主因，而平台应急响应机制（如 30 分钟启动、24 小时修复）侧重事后处理，事前风险评估与用户主动防御工具（如“一键冻结”功能仅少数平台提供）不足。

1.3 数据使用中：算法歧视与权利失衡

数据驱动的算法决策引发了系统性公平危机。

精准画像的隐性歧视，平台通过消费记录、设备型号等构建“消费潜力”标签，实施“大数据杀熟”（如老用户商品定价高于新用户），87.53%用户未察觉价格差异。更隐蔽的是，外卖平台根据支付记录推断收入水平、社交平台点赞行为被纳入信贷风控，形成跨场景“歧视链”，如低收入群体被自动过滤高价酒店推荐，构成数字时代的隐性排斥。

算法黑箱与用户控制缺失，算法决策过程不透明（如淘宝未披露动态定价模型参数），用户仅能获取基础订单信息，无法验证推荐合理性。同时，平台通过“锁定效应”强化控制——用户因社交关系、使用习惯等难以更换平台，被迫接受算法操纵。典型如，抑郁症患者被精准推送高价保健品广告，平台利用用户情感弱点牟利，突破伦理底线。

维权障碍与责任模糊，个人信息侵权案件面临证据收集难（如算法歧视举证需专业技术支持）、赔偿低（损失难以量化）、责任划分不明确（第三方共享数据时主体追责模糊）等问题，法律救济滞后于技术滥用速度，用户实质处于“被数据控制”的被动地位。

2 电商平台个人信息保护的制度性缺陷

2.1 法律制度：从框架构建到实施断层

我国已形成以《个人信息保护法》为核心的“法律+标准+监管”治理体系，覆盖信息收集、使用、跨境流动等全流程。然而，立法在技术适配与权益救济上存在显著短板：

收集环节存在规范冲突与界定模糊的问题，《网络安全法》、《电子商务法》等对“同意”标准的界定不一致，导致企业合规操作混乱。新兴技术场景（如 AI 生成虚假身份信息收集）缺乏针对性规范，法律对“最小必要”原则的量化标准缺失，加剧超范围采集风险。此外，多部法律对个人信息内涵的定义不统一，民事、行政、刑事责任衔接不畅，用户面临“多头侵权、追责无门”困境。

使用环节存在监管滞后与技术脱节的问题，算法推荐、数据跨境传输等领域存在监管真空。《互联网信息服务算法推荐管理规定》禁止价格歧视，但监管部门缺乏实时监测工具，“大数据杀熟”等行为隐蔽性强，难以取证。数据跨境传输需同时通过国家安全评估和个人权益影响评估，但两部法律审查标准不统一，企业合规成本高且风险防控割裂。

责任与救济过程中存在认定模糊与程序障碍，民事赔偿标准模糊，精神损害赔偿缺乏细则，多人侵权责任划分不清，用户维权成本高（如杭州某案例维权耗时 14 个月，成本超赔偿金额）。刑事处罚中，企业违规成本与收益严重失衡（如 CNKI 被罚款仅占年利润 1.5%），威慑力不足。程序法层面，个人信息保护公益诉讼条款缺失，检察机关、消费者协会因缺乏强制调查权，难以追究大规模侵权责任。

2.2 行政监管：从职能分散到效能弱化

监管体系存在“九龙治水”格局，独立机构缺失、标准软化、处罚失衡等问题突出：

第一，在监管体制方面存在职能分散与专业缺位的问题。我国未设立独立个人信息保护行政机构，监管职能分散于网信办、市场监管总局等多部门，权责交叉导致执法尺度不一。对算法歧视、深度伪造等新型侵权，部门因专业能力不足出现监管真空，如“大数据杀熟”行为长期因定性分歧难以有效遏制。

第二，在管理标准方面存在推荐性规范的执行困境。国家标准（如《个人信息安全规范》）缺乏法律强制力，企业选择性合规普遍。欧盟 GDPR 将标准上升为法律，违规可处年营业额 4%罚款，而我国违规企业仅面临象征性处罚，标准实施效果依赖企业自觉，技术防护措施（如加密技术）落实不到位。

第三，在处罚机制方面存在成本低廉与裁量失衡的问题。行政处罚力度与违法收益脱节，如某数据公司非法获利数千万仅罚款 200 万元，企业将处罚视为“经营成本”。罚款标准弹性大，未与企业规模、危害程度挂钩，地方保护主义导致头部企业处罚“避重就轻”，削弱法律威慑力。

第四，在监管流程阶段，存在事前备案、事中监管与事后执行的漏洞。事前备案流于形式，企业提交虚假信息即可通过；事中依赖人工审核，技术手段滞后，难以及时发现日均百万级数据违规；事后处罚执行不到位，部分企业拖延履行，监管部门缺乏强制执行手段，多元主体责任划分不清加剧追责困难。

2.3 行业自律：从规则失范到监督失效

第一，在规则制定层面存在程序封闭与利益失衡的困境。行业协会制定自律规范时，消费者参与机制缺失，规则多由企业主导，内容偏向商业利益。如某电商协会《个人信息处理自律规范》对“必要信息”界定模糊，未设违规惩戒措施，沦为形式化宣言。

第二，在监管执行过程中存在约束力弱与标准差异。自律组织缺乏强制执行力，对违规企业仅能劝告、通报，企业选择性执行核心条款（如超范围收集用户地理位置信息）。执行标准不统一，不同企业对“用户信息删除权”落实差异大，用户权益保护效果参差不齐。

第三，在外部监督方面存在独立性不足与资源匮乏的情况。法律要求的外部监督机构（如独立委员会）多由行业内专家组成，利益关联导致监督形式化。第三方认证机构、消费者协会等因缺乏技术工具和强制调查权，难以处理算法歧视等新型侵权，公众投诉常因证据不足不了了之，监督效能严重受限。

综上，电商平台个人信息保护的困境，本质是技术创新与制度供给的失衡。法律体系需从碎片化走向体系化，明确技术应用边界与责任认定标准；监管机制需通过设立独立机构、强化标准强制力，破解“罚不严、管

不住”难题；行业自律需引入公众参与、构建刚性执行与透明监督机制。唯有推动法律规制、行政监管、行业自律的协同联动，才能在数字经济发展与个人权益保护间实现动态平衡，构建“技术赋能、规则清晰、多元共治”的治理新格局。

3 电商平台中个人信息保护协同治理体系的构建

3.1 完善利益平衡的法律制度：场景化立法与技术合规双轮驱动

首先，针对跟踪定位技术滥用，立法应明确“时空关联性”判断标准，将实时位置追踪列为需用户单独授权的高风险行为，参考欧盟 GDPR 要求全链条脱敏处理，违规者面临罚款与公示惩戒。针对隐私协议形式化，建立“分级披露制度”，将协议内容分为基础信息、扩展授权、高风险行为三级，强制平台以弹窗、图文等显著方式提示用户，并设置“30 秒冷静期”防止误操作，引入第三方“隐私协议简化指数”认证倒逼企业优化披露。针对大数据杀熟，确立“价格歧视算法备案审查制度”，要求平台提交算法代码、公平性测试报告等材料，由多部门联合审查，同时强制显示“基础价格”与“个性化溢价”分项，借鉴美国 CCPA 禁止歧视性定价并设定高额罚款。

其次，扩大公益诉讼原告资格，赋予消费者协会、检察机关等组织直接起诉权，实行举证责任倒置，由平台承担数据处理合法性举证义务，并处以惩罚性赔偿与信用惩戒联动。建立“算法责任保险”制度，强制平台为数据算法投保，保费与风险等级挂钩，通过市场机制分散风险并倒逼算法伦理建设。推动区块链技术在证据存证、理赔流程中的应用，构建“公益诉讼+保险赔付+信用惩戒”的全链条救济体系。

3.2 强化全链条行政监管：独立机构与动态处罚协同发力

设立直属国务院的独立个人信息保护监管机构，统筹政策制定、执法监管与纠纷处理，整合多部门资源，解决“九龙治水”问题。要求大型平台设立外部独立监督机构，由第三方专业组织对隐私政策、数据安全进行审计并公开报告，形成“政府监管—平台自治—社会监督”的立体化制衡机制。

将《个人信息安全规范》等推荐性标准转化为法律强制要求，明确企业违反技术标准需承担民事、行政甚至刑事责任，授权监管部门动态修订标准并作为司法裁判依据。建立全国统一备案系统，引入 AI 核验与第三方技术评估，确保备案真实性；开发实时监管平台，运用大数据、区块链技术实现数据处理全流程监测，破解“技术规避”难题。

借鉴欧盟 GDPR“阶梯式”处罚模式，将罚款与企业年营业额、违法情节挂钩，设置最低罚款下限，明确从轻/从重处罚情形，避免“过罚不当”。强化中央垂直执法，破除地方保护主义，将处罚结果纳入企业信用体系，限制融资、招投标等活动，推动“认罚”向“合规”转化。

3.3 健全系统规范的行业自律：多元参与与救济渠道创新

第一，行业协会制定自律规范时，需公开征求意见、召开听证会，邀请消费者、专家参与，避免企业主导的利益失衡。建立动态反馈机制，结合技术发展与公众需求定期修订规则，确保“必要信息”等关键条款可量化、可操作。

第二，设立独立监督委员会，联合第三方机构开展合规审计与认证，将结果与企业信用挂钩。开发区块链监管平台，通过智能合约自动监测超范围收集等违规行为，触发预警并提交监管部门。推动自律规范与法律监管数据共享，形成“自律预警—监管介入”的协同响应。

第三，设立行业调解机构，参照韩国模式制定标准化流程，15 个工作日内处理用户投诉，调解协议具约束力；探索行业仲裁机制，允许用户与企业约定仲裁解决纠纷，裁决结果可纳入失信名单。畅通“一站式”投诉平台，公示处理进度并引入满意度评价，对多次违规企业采取公开谴责、暂停会员资格等措施，强化救济手段的强制性。

参考文献

[1]张基利,康兰平.电商平台中公民个人信息保护规范路径探讨——基于 APP 隐私政策的实证研究[J].现代商贸工业,2022(21):181-183.
[2]刘春,奉其其,祝嘉悦.中国应用软件中数据可携带权的实证分析[J].天府新论,2025(2):41-52.
[3]程啸.论个人信息侵权责任中的违法性与过错[J].法制与社会发展,2022(5):191-209.
[4]张继红.大数据时代个人信息保护行业自律的困境与出路[J].财经法学,2018(6):57-70.
[5]候姝琦,程雪军.大数据时代个人信用信息权益的法律保护缺位与完善[J].征信,2022(9):25-34.

作者简介：潘煜萌（1998.3），女，蒙古族，内蒙古阿拉善左旗人，硕士，北方民族大学，研究方向：法律