

网络购物平台用户数据保护的法律挑战与治理新路径

朱沁春

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年6月9日; 录用日期: 2025年6月23日; 发布日期: 2025年7月15日

摘要

网络购物平台用户数据兼具人格权益与经济价值属性, 个人信息与隐私存在交叉易导致责任竞合。当前数据保护面临多重困境, 收集环节存在超范围收集、捆绑式授权和隐性收集问题; 共享流转环节透明度不足、责任界定模糊, 跨境流动监管缺失; 数据泄露侵权时, 责任主体认定难、损害量化阻碍大且司法救济成本高。法律责任体系中, 民事责任采用“过错推定 + 举证责任倒置”, 行政责任需优化裁量基准, 刑事责任实现从个人到单位追责转变, 同时应落实数据全生命周期保护要求。为完善保护, 需构建精细化数据分类管理体系, 保障用户权利, 完善动态监管与应急响应, 提升全民数据素养, 强化平台义务, 建立全链条责任体系, 以实现用户权益保护与数字经济发展共赢, 并推动形成符合国情的用户数据保护范式。

关键词

网络购物平台, 用户数据保护, 法律责任, 个人信息, 数据治理

Legal Challenges and New Governance Paths for User Data Protection on Online Shopping Platforms

Qinchun Zhu

Law School of Guizhou University, Guiyang Guizhou

Received: Jun. 9th, 2025; accepted: Jun. 23rd, 2025; published: Jul. 15th, 2025

Abstract

User data on online shopping platforms has dual attributes of personality rights and economic value. The overlap between personal information and privacy can easily lead to liability concurrence.

文章引用: 朱沁春. 网络购物平台用户数据保护的法律挑战与治理新路径[J]. 电子商务评论, 2025, 14(7): 1095-1101.
DOI: 10.12677/eci.2025.1472278

Current data protection faces multiple dilemmas: in the collection phase, there are issues of excessive data collection, bundled authorization, and implicit data collection; in the sharing and circulation phase, there is insufficient transparency, vague liability definition, and lack of cross-border flow supervision; when data leakage occurs, it is difficult to identify responsible entities, quantify damages, and the cost of judicial relief is high. In the legal liability system, civil liability adopts “presumption of fault + inversion of the burden of proof”, administrative liability needs to optimize discretion benchmarks, criminal liability shifts from individual to unit accountability, and full lifecycle data protection requirements should be implemented. To improve protection, it is necessary to build a refined data classification management system, safeguard user rights, improve dynamic supervision and emergency response, enhance public data literacy, strengthen platform obligations, and establish a full-chain liability system, so as to achieve a win-win situation between user rights protection and digital economic development, and promote the formation of a user data protection paradigm that suits national conditions.

Keywords

Online Shopping Platforms, User Data Protection, Legal Liability, Personal Information, Data Governance

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

根据 2024 年发布的《中国新电商发展报告》数据显示, 2023 年中国网络零售市场呈现稳健增长态势, 全国网络零售总额达 15.42 万亿元, 较上年增长 11%, 自 2013 年起已连续 11 年保持全球网络零售市场首位。值得关注的是, 网上实物商品零售额在社会消费品零售总额中的占比持续提升, 已达 27.6%, 充分体现电子商务在拉动国民消费增长中的重要作用。作为新电商领域的核心构成, 新电商市场规模在 2023 年突破 4.9 万亿元, 同比增长了 35.2% [1]。充分展示了其在激发消费潜力、引领市场新风向中的核心作用。平台经济的繁荣依赖于用户数据的深度开发, 但近年来“大数据杀熟”“数据泄露”“过度收集信息”等事件频发, 暴露出数据利用与权利保护的失衡。鉴于 2021 年施行的《个人信息保护法》, 我国用户数据保护已经进入法典化时代, 但网络购物场景中数据处理的复杂性, 对于法律责任认定存在很多模糊地带。本文从数据属性的双重性出发, 系统分析保护现状、现实困境及优化路径, 以期为构建契合数字经济发展规律的用户数据保护体系提供理论支撑。

2. 网络购物平台用户数据保护的必要性

(一) 数据属性的双重价值驱动

用户数据具有人格权益与经济价值的二元属性。在大数据时代个人信息已经成为一种经济资源, 在利益驱动下, 各种非法收集、买卖、窃取等滥用个人信的行为屡禁不绝[2]。在人格权益维度, 姓名、身份证号、生物特征等直接识别信息, 以及浏览记录、消费偏好等间接识别信息, 均构成自然人的“数字人格”要素, 与人格尊严、隐私安全及自主决定权密切相关。我国《中华人民共和国民法典》(以下简称《民法典》)第 1032 条将私密信息纳入隐私权保护范畴, 第 1034 条明确个人信息的法律保护地位, 凸显数据作为人格利益载体的重要性。在经济价值维度, 用户数据是平台精准营销、产品研发、商业模式创新的核心生产要素。双重属性决定了用户数据保护不仅是保障基本人权的法治要求, 更是维护数据要素

市场有序运行的必要前提。

(二) 侵权风险的现实紧迫性

当前平台数据侵权呈现规模化、技术化、跨国化趋势。国家互联网应急中心数据显示，2023 年全国受理网络数据安全投诉举报超 28 万件，其中购物平台占比达 35%。典型侵权形态包括：过度收集用户生物特征信息用于商业分析，非法共享交易数据导致用户隐私泄露，数据跨境传输未履行安全评估义务引发监管风险等。例如，某电商平台因违规收集用户短信验证码被工信部处以 100 万元罚款；某跨境电商平台因数据存储在境外服务器遭黑客攻击，导致数百万用户地址、支付信息泄露。此类事件不仅侵害用户隐私权、财产权，更可能引发电信诈骗、精准钓鱼等次生风险，数据保护已成为维护网络空间安全的核心议题。

3. 网络购物平台用户数据的现有保护手段

(一) 法律规范构建责任体系

在各种维权方式中，法律法规因其自身特有的权威性、有效性和强制性，成为维护合法权益的重要途径[3]。

(1) 民事责任：过错推定与举证责任倒置

《个人信息保护法》规定个人信息侵权责任为过错推定责任，这是因为在信息处理活动中，一般情况下信息主体相较于网络平台等处理者处于弱势地位，处理信息的具体情况和相关证据通常只有处理者才能掌握[4]。信息处理规定数据处理者不能证明自己无过错的，应当承担损害赔偿责任。司法实践中，用户只需证明数据泄露事实与平台安全漏洞存在时空关联性，即可推定因果关系成立，显著降低维权门槛。例如，某用户因平台账号被盗导致资金损失，法院依据平台未履行数据加密义务的技术鉴定报告，判决其承担全额赔偿责任，体现了对弱势群体的倾斜保护。《民法典》第 1034 条：自然人的个人信息受法律保护；《民法典》第 1035 条规定：处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理。上述条文分别确立了个人信息的民事权利属性，以及处理原则。

(2) 行政责任：阶梯式处罚与信用惩戒

市场监管构建三级处罚体系：对隐私政策未及时更新等轻微违法，处最高 100 万元罚款；对非法共享数据、跨境传输违规等严重违法，处上一年度营业额 4% 以下罚款，可并处停业整顿；对累犯企业，对直接责任人处 10~100 万元罚款。2023 年某平台因非法出售用户地址信息，被处以年营业额 3% 的罚款(约 2.1 亿元)，并列入失信企业名单，彰显“处罚到人、信用联动”的监管威慑力。

(3) 刑事责任：单位犯罪认定与入罪标准细化

《中华人民共和国刑法》第 253 条之一“侵犯公民个人信息罪”明确量化入罪标准，提供 50 条以上轨迹信息或 500 条以上交易数据即可追究刑事责任。“拒不履行信息网络安全管理义务罪”将责任主体扩展至单位，2023 年某电商平台因未及时修复数据漏洞导致大规模泄露，被判处单位罚金 500 万元，相关技术负责人被判处有期徒刑 3 年，体现了“双罚制”的立法导向。

(二) 技术措施筑牢安全防线

平台普遍应用多层级技术防护体系：在数据存储环节，对身份证号、金融账户等核心数据采用 AES-256 国密算法加密，部署专用物理服务器并实施访问权限最小化管理；在权限控制环节，通过 RBAC(角色基于权限控制)系统，将敏感数据访问权限限定于 3 人以内的安全团队；在数据共享环节，运用隐私计算技术实现“数据可用不可见”，如联邦学习技术使多方数据在本地加密处理后，仅向合作方提供脱敏聚合结果，从技术层面阻断身份关联风险。

(三) 行业自律提升保护标准

2022 年《电子商务平台用户数据保护自律公约》建立分级保护机制，要求年处理 10 亿条以上数据的平台设立独立数据保护委员会，由外部独立董事担任负责人，并且规定每季度需公开《数据安全评估报告》。2023 年，中国网络空间安全协会推动建立第三方认证制度，对平台数据收集合法性、共享的合规性进行审计，引导行业从“最低合规”向“最佳实践”升级，形成法律规制与行业自治的协同治理格局。

4. 网络购物平台用户数据保护的现实困境

网络购物作为数字经济下的购物新形式，对于规则制定、司法救济以及外部监督等方面法律法规的规定和保护都处于起步与完善阶段[5]，这使得用户数据保护存在着现实困境。

(一) 规则建构粗放：法律要件模糊化困境

一方面，“同意”规则亟待健全。虽然《个人信息保护法》规定了单独同意和书面同意等一些新形式，并对相应的适用场景也进行了规定。但遗憾的是，并没有进一步解释单独同意、书面同意的具体含义，这与传统民法中的民事同意是一个等同概念抑或是标准更高的概念，需要立法进一步释明。另一方面，敏感信息的处理规则需要进一步完善。《个人信息保护法》在敏感信息处理规则方面仍然不够精细，难以适应现实中个人信息的复杂性[6]。

(二) 数据控制失衡：收集环节的技术滥用困境

(1) 超范围采集数据

部分平台以“提升服务体验”为名，实施过度收集行为。某购物 App 强制获取用户通讯录权限，美其名曰“方便推荐亲友喜好商品”，实则用于构建社交关系图谱以精准锁定消费群体；某生鲜平台在用户未启用定位功能时，通过设备传感器持续采集位置信息，用于区域消费热力分析。第三方测评显示，83%的购物类 App 存在“非必要信息收集”问题，严重违反《个人信息保护法》“最小必要”原则，构成对用户自主决定权的侵害。

(2) 捆绑式授权与格式条款霸权

平台普遍设置“不同意则无法使用”的刚性条款，用户注册时若拒绝勾选包含多项非必要授权的隐私政策，将被禁止进入购物流程。这种“强制缔约”的模式剥夺了用户的选择权，形成“数字霸权”困境。2023 年某平台因隐私政策中“授权条款不可拆分”问题，被市场监管总局认定为违反《消费者权益保护法》，反映出格式条款规制的现实紧迫性。

(3) 隐性收集与技术黑箱操作

借助 Cookies、设备指纹等技术，平台在用户无感知状态下收集浏览轨迹、设备信息等数据。例如，用户浏览母婴商品页面时，系统自动记录停留时长、点击频次等行为数据，经算法整合后用于个性化推荐，但用户难以察觉此类数据收集行为，导致知情权落空。技术的隐蔽性使得用户对数据处理过程缺乏有效控制，形成“数据收集黑箱”。

(三) 数据共享流转：透明度缺失与责任虚化

(1) 第三方合作中的安全漏洞与责任推诿

平台与物流、支付、营销等第三方机构合作时，普遍存在授权链条模糊、安全审查缺位问题。某平台向物流合作方提供用户地址信息时，未限定数据使用范围，导致信息被违规转卖；某支付机构因数据接口安全设计缺陷，导致百万条支付记录泄露，涉事双方互相推诿责任，用户陷入“维权无门”境地。这种多主体参与的数据处理模式，使得侵权责任认定陷入碎片化困境。

(2) 跨境流动监管真空与法律管辖冲突

跨境电商平台将用户数据存储于境外服务器或向境外传输时，常未履行《数据安全法》规定的跨境安全评估义务。由于各国数据保护标准差异显著——欧盟《通用数据保护条例》(GDPR)要求数据本地化

存储,美国采用行业自律主导的分散化监管模式,我国用户数据在境外面临监管规则不统一、司法救济难以实施等问题。2023 年某跨境平台因数据境外泄露,用户在国内法院起诉时遭遇管辖权争议,暴露跨境数据治理的制度短板。

(四) 数据泄露救济: 责任认定复杂与赔偿机制滞后

(1) 多元主体责任划分难题

数据泄露可能源于平台技术漏洞、员工职务行为、第三方过失等多重因素,责任主体认定存在复杂性。2023 年某平台员工私自出售用户数据,平台以“个人行为”为由拒绝承担责任,用户需举证证明平台存在管理失职,举证难度高、周期长,反映出职务行为与个人行为的法律边界模糊问题。

(2) 损害后果举证困难

数据泄露的损害后果具有隐蔽性与延展性:直接经济损失(如资金盗刷)相对容易举证,而隐私泄露导致的精神损害、信用评价降低等间接损失,因缺乏量化标准和举证规则,难以获得司法支持。2022 年某用户因数据泄露遭遇持续骚扰电话,起诉索赔精神损害赔偿,法院以“未达到严重后果”为由驳回诉求,凸显现行法律对非财产损害救济的局限性。

(3) 网络用户维权艰难

消费者在网络购物时难以获取和保留自身消费行为和权益受到侵害的有效证据,导致维权困难[7]。民事诉讼中,用户需承担技术鉴定、证据公证等高昂费用,而平台利用信息优势拖延诉讼,导致维权周期长达 1~2 年。行政监管方面,部分平台罚款仅占年营业额 0.1%,违规成本低于合规成本,难以形成有效震慑,反映出“违法获益大于守法成本”的制度失衡。

5. 网络购物平台用户数据保护的解决路径

针对上述结构性困境,需建立“规则细化-流程控制-监管创新-救济优化”的闭环治理体系,实现对数据生命周期的精准干预:

(一) 破解规则粗放: 构建精细化法律要件体系

(1) 明确“同意”规则的操作细则

界定“单独同意”需满足“授权界面独立、条款可分项勾选、撤回操作便捷”三要件,禁止将核心功能使用与非必要授权捆绑;规定“书面同意”包括电子签名、生物特征确认等可信形式,明确未成年人、老年人等特殊群体的差异化同意规则,如监护人二次确认规则。

(2) 建立敏感信息动态分级保护制度

将用户数据分为三级:核心数据(生物特征、金融账户)需单次单项授权 + 活体检测;重要数据(地址、交易记录)需去标识化处理 + 使用期限限制;一般数据浏览记录采用默认拒绝收集模式。要求平台对敏感信息处理进行年度风险评估,第三方机构出具合规审计报告方可继续使用。

(二) 矫治收集失衡: 建立透明化控制机制

(1) “最小必要”原则的技术化实施路径

构建智能化权限监测系统,通过自动化算法对 App 收集的数据与核心业务功能的关联性进行深度分析,对超出必要范围的权限申请触发警示机制,例如,当购物类 App 申请调用相机权限时,系统即时弹出包含详细使用说明的交互界面。

开发用户数据可视化管理平台,动态展示数据采集类别、使用频率等关键信息,并量化呈现权限调整对业务功能的影响,同时提供分级权限管理功能,支持用户灵活选择数据授权范围,实现权限撤回与核心功能保留的兼容。

(2) 格式条款治理的程序正义优化方案

建立分级授权机制：对基础业务功能(商品展示、订单提交等)采用概括授权模式；对增值服务功能(社交分享、个性化推荐等)实施分项授权；对涉及生物特征等敏感信息的功能如人脸识别支付，要求用户通过生物识别与密码双重验证完成授权。

制定平台隐私政策负面清单制度，明确划定数据采集禁区，严禁收集通话记录、短信内容等非必要信息，并将违规行为纳入企业信用评价体系，实施失信惩戒措施。

(三) 填补流转漏洞：构建全链条责任追溯体系

(1) 第三方合作的授权链硬化

强制签订《数据共享责任承诺书》，明确合作方数据使用范围如物流方仅限配送使用地址信息、保存期限在配送完成后 72 小时删除、泄露赔偿不低于损失 3 倍的违约责任；运用区块链技术建立数据流转台账，记录每次共享的时间、接收方、用途等信息，实现“数据流向可追溯、责任主体可锁定”，2023 年某试点平台通过该技术将责任认定周期从 180 天缩短至 7 天。

(2) 跨境流动的监管规则衔接

建立“出境评估 + 认证互认”机制：向欧盟传输数据需通过 GDPR 等效性评估，向美国传输需通过“中美数据安全认证”，未通过评估的平台禁止跨境传输；设立境外数据监管专员，要求平台定期报告境外数据存储位置、安全措施及泄露处置情况，违反者处上年营业额 1%~5% 罚款。

(四) 优化救济机制：创建低成本高效能维权通道

(1) 多元主体责任的举证责任倒置

明确“数据处理者不能证明自身无过错的，推定其对员工行为、合作方过失承担连带责任”，减轻用户举证压力。例如，在员工销售数据案件中，平台需证明已履行岗位权限隔离、定期安全培训等义务，否则直接承担赔偿责任。

(2) 损害救济的立体化建构

建立“基础赔偿 + 精神补偿”的双轨制：直接损失按实际金额赔偿，精神损害采用“定额赔偿 + 情节浮动”的赔偿方法，如骚扰电话侵权可主张 2000~10,000 元赔偿；推行“行政罚款转救济基金”制度，将平台缴纳的罚款 30% 纳入用户维权专项基金，用于补贴技术鉴定、公证等费用，2024 年某省试点基金已覆盖 80% 的维权成本。

(3) 完善动态监管与应急响应

提高网络服务市场的监管效能，充分发挥政府职能，根据违法情形的不同，采取不同的处罚措施[8]。监管部门应建立“风险评估 - 分级监管 - 持续改进”的监管机制，对处理超百万用户数据的平台实施季度安全审计。要求平台制定完善的数据泄露应急响应预案，明确规定在数据泄露事件发生后，需在 1 小时内向相关部门报告、72 小时内通知受影响用户，并定期组织应急演练。积极探索建立“监管沙盒”(监管沙盒是由监管机构提供一种被控制的实验环境，其允许新兴产业或技术在监管的范围内进行创新但不致于引发系统风险，监管机构可以实时监测并管理相关风险，而企业也无须立即承担因违法而产生的监管责任机制[9])，允许新技术在可控环境中验证数据安全性能。

通过上述路径，可实现从“问题导向”到“系统治理”的转变，在法律规则、技术措施、监管机制三个维度形成协同效应，最终破解网络购物平台用户数据保护的现实困境，构建权益保障与产业发展并重的数字治理新生态。

6. 结论

网络购物平台的用户数据保护，本质上是数字经济时代权利配置与利益平衡的系统性工程。我国当前已构建起“法律规制 + 技术赋能 + 行业自律”的多维保护框架，但在规则细化、责任落实与技术创

新等方面仍需突破。未来,需进一步强化平台作为“数据受托人”的法律义务,建立“风险预防-过程控制-损害救济”的全链条责任体系,同时兼顾数据开发利用与产业创新,最终实现用户权益保护与数字经济发展的共赢。在全球数据治理规则加速重构的背景下,我国应积极参与国际规则制定,推动形成符合中国国情的用户数据保护范式,为数字经济健康发展奠定坚实的法治基础。

参考文献

- [1] 中国网络社会组织联合会, 中国国际电子商务中心. 中国新电商发展报告[R]. 2024.
- [2] 吴清烈. 电子商务法治时代大数据应用与个人信息保护[J]. 人民法治, 2019(5): 22-25.
- [3] 冯梦飞. 电子商务时代的消费者权益保护——跨境在线购物的法律挑战[J]. 互联网周刊, 2023(19): 48-50.
- [4] 蒋薇薇. 个人信息侵权责任探究——以请求权基础为中心[J]. 东南大学学报(哲学社会科学版), 2024, 26(S2): 126-129.
- [5] 孙文红. 司法服务保障数字经济发展的路径与对策[J]. 沈阳工业大学学报(社会科学版), 2022, 15(2): 179-183.
- [6] 高志宏. 数字经济时代个人信息的识别标准及规范续造[J]. 社会科学辑刊, 2023(2): 68-77.
- [7] 张谪馨. 网络购物纠纷的成因、困境及法律解决途径[J]. 知与行, 2024(1): 63-71.
- [8] 庄园. 网络购物中对消费者权益的保护[J]. 广西质量监督导报, 2020(7): 268-269.
- [9] 张肇廷, 李轩. 大数据监管: 运行逻辑、风险议题与规制进路[J]. 广东财经大学学报, 2024, 39(6): 103-111.