E-Commerce Letters 电子商务评论, 2025, 14(11), 3219-3225
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113799

Hans汉斯

浅论数据确权背景下网络营销的合法边界

杨斡旋

贵州大学法学院，贵州 贵阳

收稿日期：2025年10月14日；录用日期：2025年10月28日；发布日期：2025年11月28日

摘 要

在数据产权“三权分置”框架落地以及《数据安全法》《个人信息保护法》深入施行的背景当中，第三方数据共享已然成为网络营销领域里精准触达用户提升效率的关键模式。在网络营销实践中“新浪微博诉脉脉”案所确立的“三重授权”原则遭遇诸多适用难题，诸如用户授权有效性模糊，平台授权边界不清晰数据流转权责出现脱节等情况。这不仅导致企业合规风险大幅加剧，而且对用户信息权益造成了侵害，在网络营销中第三方数据共享用于营销，是个典型疑难场景。本文围绕“三重授权”原则，把电商经济领域核心期刊文献同司法案例相结合，深入分析原则适用困境，构建具有针对性的合法边界体系与解决策略。这为网络营销中第三方数据共享的合规实践，给予理论支撑与操作指引。

关键词

数据确权，网络营销，个人信息保护，算法治理

A Brief Discussion on the Legal Boundaries of Online Marketing under the Background of Data Ownership

Woxuan Yang

School of Law, Guizhou University, Guiyang Guizhou

Received: October 14, 2025; accepted: October 28, 2025; published: November 28, 2025

Abstract

Amid the full implementation of the Data Security Law and the Personal Information Protection Law, and the rollout of the “three-right split” regime for data property, third-party data-sharing has become the pivotal tool for precision targeting and efficiency gains in online marketing. In practice, however, the “triple-consent” rule forged in Weibo v. MaiMai is colliding with serious friction: the

文章引用: 杨斡旋. 浅论数据确权背景下网络营销的合法边界[J]. 电子商务评论, 2025, 14(11): 3219-3225.
DOI: 10.12677/ecl.2025.14113799

validity of user consent is blurred, the scope of platform consent is undefined, and data-flow responsibilities are decoupled. These gaps sharply raise corporate-compliance risk and erode users' information rights. Focusing on marketing-oriented third-party data-sharing—the most contentious scenario—this paper uses the triple-consent rule as its axis, synthesizes core e-commerce journal literature with leading court decisions, dissects the rule's operational dilemmas, and constructs a tailored legitimacy-boundary system plus remedial strategies, offering both theoretical grounding and a practical playbook for compliant data-sharing in online marketing.

Keywords

Data Ownership Verification, Online Marketing, Personal Information Protection, Algorithm Governance

1. 引言

数字经济时代，数据已成为全球公认的核心生产要素。网络营销作为数字经济的新兴领域，其早已从传统的“广而告之”变为对用户画像和行为预测为内容的“数据驱动”模式。然而，据相关统计，2024年电商行业通过第三方数据共享实现的营销转化率较传统模式提升 35% [1]，第三方数据共享(像电商平台与营销服务商、社交平台之间关于用户消费偏好浏览行为数据的共享)，能够显著优化用户体验提升广告投放精准度。

我国出台了《网络安全法》《数据安全法》《个人信息保护法》等一系列法律以应对上述困境，由此构建的法律体系将我国以该体系为核心的监管短板有效弥补。此举彰显了我国对数据利用监管力度的强化，尤为关键的是《关于构建数据基础制度更好发挥数据要素作用的意见》提出的数据产权“三权分置”框架，其目的在于破解数据确权难题进而为数据要素的市场化流通奠定制度基础。

在此情形下，一个关键问题凸显：在数据权利归属逐渐清晰明确的情形下，企业网络营销的合法边界该如何予以界定？过往传统研究大多将视角局限于从《广告法》《反不正当竞争法》或者《消费者权益保护法》的单一维度来展开剖析，然而并没有在数据确权这一意义重大的制度变革背景环境下针对网络营销展开具有系统性且全面性的考察。

现有研究大多围绕数据确权二元结构，或者针对网络营销全流程风险展开宏观探讨，丁晓东(2021)基于个人信息保护原理，对数据处理里的权利边界展开了分析[2]；申卫星在 2020 年将关注点放在数据用益权上，对企业数据产权的实现路径展开了探讨[3]。

但针对第三方数据共享营销场景中“三重授权”原则适用困境的专项研究较为匮乏，且文献引用多集中于法律领域，对电商经济实践中的具体问题结合不足。本文立足电商营销实践，整合电商经济与数据法律领域核心文献，深入挖掘“三重授权”原则的适用痛点，填补该细分领域研究空白，为企业合规与监管实践提供参考。

2. 数据确权的法律内涵与二元结构

《数据安全法》定义数据为：“任何以电子或者其他方式对信息的记录。”因此从法律定义的角度看，数据和信息两者是密不可分的，有着一体两面的形态。但是在经济学上，只有当数据融入到人类的

劳动中，并能够发挥经济效益时，它才能称得上生产要素。马克思曾指出，劳动生产力受到工人的技能水平、科学发展程度、生产过程的社会组合、生产资料的规模和效能以及自然条件等多种因素的影响。如此说来，数据是通过影响科学的发展和应用来实现劳动生产力的提升。总体上讲，数据作为现代社会的新型生产要素，一方面是非物质性的数字劳动生产活动的产物，另一方面也具有使用价值和价值。数据不但给数字经济时代的社会发展带来了全新的动力，还在推动社会生成新的生产关系。在现代化的背景下，数据这种新型生产要素的加入，给中国经济的转型发展产生了很深远的影响。中国式现代化的不仅仅是要求满足物质财富的增长，同时还要求注重社会的和谐稳定和可持续发展。在这段过程中，数据作为关键的生产要素，一定会在推动经济结构的完善、促进产业的转型升级和加强社会的管理和服务能力这些方面发挥重要且不可替代的作用。在我国现行法律框架下，主要呈现出以下情形。

以个人控制为核心的个人信息权益。《个人信息保护法》第四章专章规定了“个人在个人信息处理活动中的权利”[2]，确立了一套以个人控制为核心的权利体系。这包括知情权、决定权、限制权、拒绝权、查阅复制权、可携带权、更正补充权及删除权。其法理基础源于《宪法》保障的人格尊严与《民法典》保护的隐私权，核心宗旨是赋予个人对其信息利用方式的控制力。对于网络营销而言，这意味着任何商家或主播对个人数据的处理行为，其合法性源于个人的明确授权，否则便构成侵权。

以利益导向为目标的企业数据产权。由于单纯的个人控制无法充分释放数据作为生产要素的经济价值。为此，“数据二十条”创新性地提出建立数据资源持有权、数据加工使用权、数据产品经营权“三权分置”的产权运行机制[3]。具体如下：

1. 数据资源持有权：指企业对依法收集形成的数据资源持有并予以管控的权利。

2. 数据加工使用权：指企业通过投入技术、资本和劳动，对原始数据进行深度加工处理的权利。

3. 数据产品经营权：指企业对经过深度加工形成的具有预测性和营利性的数据产品和服务享有经营、收益和处分的权利。

这一框架在司法实践中已得到认可。在著名的“淘宝诉美景”案[3]中，法院认定淘宝公司开发的“生意参谋”数据产品，系其投入巨大研发成本形成的结果，而美景公司直接抓取使用该产品内容，实质性替代了原告提供的服务，构成了不正当竞争。此案确立了“投入－产出”规则，为企业对其衍生数据产品主张权益提供了法理依据。

由此可见，数据确权构建了一个相对规范的二元结构：一端是侧重于保护的个人信息权益，另一端是侧重于利用的企业数据产权。网络营销的合法性，正取决于其行为是否能够同时尊重这两端的权利，并在其划定的范围内运行。任何越界行为，都将面临相应的法律风险。

3. 网络营销的数据实践与法律风险

企业常以“概括授权”替代“具体授权”，如隐私政策中表述为“同意平台将数据用于营销相关目的”，未明确“第三方共享”的具体场景。实践中，企业多采用“弹窗勾选”“默认同意”等形式获取授权，但《个人信息保护法》要求“单独同意”需具备“主动确认”特征。

同时，多数企业未提供便捷的授权撤回渠道，部分平台需用户通过“客服申请－人工审核－7 个工作日反馈”等复杂流程撤回授权，违反《个人信息保护法》“撤回与同意同等便捷”的要求。

网络营销的全流程可以被看作一个完整的对数据的价值的利用环节，其每个环节都可能触发特定的法律风险。具体如下：

其一、数据采集环节。在此环节易造成合法性基础的缺失 ，如果企业通过用户注册表单、第三方授权登录等方式收集用户数据。常见的风险包括：

“一揽子授权”与“强制同意”。App 通过“不同意就不让用”的方式，捆绑索取与当前服务无关的

权限(如通讯录、精确位置)，违反了《个人信息保护法》的“自愿、知情”原则。目的不明与过度收集：隐私政策语焉不详，未清晰告知数据收集的具体目的，或收集与实现功能无关的非必要信息。

其二、数据处理与分析环节。将用户信息私密处理以及类型化的风险。企业将收集的原始数据放入CDP (客户数据平台)进行清洗、整合，通过大数据算法勾勒出用户画像并进行标签化。而此环节的风险点在于：

每一对象是否同意。《个信法》第24条规定，利用个人信息进行自动化决策如用户画像和进行个性化推荐，应保证其透明度和结果公平，并提供不针对其个人特征的选项。实践中，许多企业未就此取得用户的单独同意。

模糊用户画像不成功。如果企业对数据的处理不符合标准，不法之徒可能通过数据融合技术实现“再识别”，还原用户信息，导致个人信息泄露，从而构成违法。

其三、数据应用环节。这是风险最为集中的环节，因为这个环节有着多重法律责任的交汇。可能同时触发民事、行政乃至刑事责任。首先是民事侵权责任，对营销商来说，未经允许的个性化广告推送、无法关闭的短信营销，构成对个人信息权益和生活安宁权的侵害。其次是行政责任，若违反《个人信息保护法》第66条，可能面临最高上一年度营业额5%的巨额罚款，如果有虚假广告，则受《广告法》规制。尤其值得一提的是不正当竞争，这是高风险区。一是非法数据抓取，如“新浪微博诉脉脉”案[1]确立的“三重授权”原则，第三方获取数据，除用户授权外，还必须获得平台授权，且不得超越授权范围。二是大数据“杀熟”，即基于用户画像实行差异性交易条件，构成价格歧视，侵犯消费者公平交易权，这种侵权行为已被多地市场监管部门处罚。三是数据垄断行为，大型平台利用其数据优势实施“二选一”、屏蔽链接等，排除限制竞争。

4. “三重授权”原则在网络营销中的适用困境

本文将基于前文提及的网络营销可能触及的种种风险，对其中“三重授权”原则的困境与解决措施展开具体阐述。

“三重授权”原则源于2016年“新浪微博诉脉脉”案(北京知识产权法院(2016)京73民终588号)的“三重授权”原则，法院清晰指出，第三方平台获取用户数据必须满足“用户授权 + 原平台授权 + 不超越授权范围”这三个重要件。该原则此后逐步被纳入国家立法与监管体系：《个人信息保护法》第23条明确规定，当个人信息处理者打算向第三方提供个人信息的时候必须取得个人的单独同意，这一规定为“用户授权”提供了坚实的法律依据。《数据安全法》第21条要求数据处理者构建数据分类分级保护制度，这在一定程度上间接强化了“原平台授权”中对于数据权属的界定需求；2023年《电商数据安全管理指引(征求意见稿)》把“三重授权”原则细化到电商领域，并进一步明确规定：电商平台要是向第三方共享用户数据，必须留存授权凭证而且使用时不能超出授权范围[4]。

从法律逻辑来讲“三重授权”这一制度设计目标核心是在推动数据要素实现流通期间，对数据滥用风险加以防范，它是用来平衡个人信息权益(用户端)企业数据产权(原平台端)以及营销效率(第三方端)。

“三重授权”原则在网络营销中的适用困境具体表现在三个方面。

(一) 用户授权：有效性认定的模糊地带

电商平台在获取用户授权时常采用“一揽子授权”表述，如隐私政策里仅写着“同意平台将数据用于营销相关目的”，却未明确“第三方共享”的具体主体数据类型以及使用期限，如此一来授权内容“概括化”导致用户知情权受损。在《电商平台中的个人信息保护研究》里潘煜萌(2025)提到电商领域仍存在

[1]北京知识产权法院(2016)京73民终588号民事判决书(新浪微博诉脉脉案)。

隐私协议形式化、定位跟踪技术滥用、算法歧视等突出问题，与《个人信息保护法》“知情同意”这一核心原则相违背[5]。

《个人信息保护法》第 23 条明确规定，向第三方共享数据时必须取得用户“单独同意”，然而在实际情况中电商平台在授权形式上存在“形式化”问题，单独同意的要件有所缺失。多采用“注册时默认勾选”，“弹窗一闪而过”等方式来规避此项义务，根据中国消费者协会发布的报告，在被测评的 100 款 App 中，59 款未明确告知收集个人信息的类型和用途，且收集敏感信息时未明确告知用户信息的用途[6]。

多数电商平台未提供便捷的授权撤回渠道，导致权利行使受阻，授权撤回“复杂化”用户需历经“客服申请–人工审核–7 个工作日反馈”等流程，才能撤回授权。并且即便撤回后平台仍未及时停止数据共享，徐伟和李文敏(2025)表明隐私政策作为 App 向用户解释收集规则并提供投诉、举报等诉求路径的主要手段，应当清晰且透明，并承担起 App 与用户之间沟通的桥梁作用，现实却是隐私政策语言晦涩并且关键信息被掩盖[7]。

(二) 平台授权：边界与权责的界定难题

电商平台与第三方签订的授权协议中，原平台授权范围呈现“模糊化”态势，此类协议常设有“兜底条款”像“授权第三方使用数据开展合法电商营销”，然而数据使用的平台范围、时间范围以及具体场景均未予以明确。这一状况使得数据滥用风险不断加剧，工信部“黑名单”显示，APP 存在着没有经过用户同意收集和使用相关的个人信息且在用户个人数据保护方面存在着安全风险，存在着第三方监管不到位的问题[8]等问题。

部分电商平台为实现营销协同通过“数据互换”开展平台间“数据互授权”操作(A 电商平台将用户数据授权给 B 社交平台使用，B 社交平台反过来授权 A 平台使用社交数据)。然而它们并未单独取得用户对于“跨平台数据共享”的同意，从本质上规避了“三重授权”原则。

(三) 流转环节：授权链条的断裂与失控

电商平台称“匿名化处理后的数据无需授权”，可数据脱敏存在“形式化”现象且授权豁免认定困难重重，某数据安全审计表明实践里“伪匿名化”问题极为突出，78%的“匿名化电商数据”能借助与“用户收货地址片段 + 购买时间”相结合，达成再识别[9]。现有法律并未明确“有效匿名化”的标准，这使得企业对于“是否需要重新授权”感到困惑。

然而随着 App 治理法律政策相继出台，个人信息保护管理职责变得更加分散复杂，职权交叉、分散执法等问题普遍存在，主要原因在于监管主体之间缺乏协调机制，职责界定不清，导致多头治理、边界模糊现象频发[10]。

5. “三重授权”原则下电商营销的合法边界建构

既然出现了这样的困境，我们就应该对“三重授权”原则下电商营销的合法边界建构做出一个综合性的框架来界定。

(一) 以“有效用户授权”为程序前提，明确授权规则

电商平台构建“场景化授权”机制时，要依据营销场景对授权内容加以拆分，以“第三方精准广告投放”场景为例，需清晰地向用户说明“数据会共享给 XX 第三方公司，用于推送 XX 品类商品广告有效期为 XX 天”，并通过“单独弹窗 + 主动点击确认”的方式来获取授权，防止出现概括授权的情况。在电商 APP 里设置“数据授权管理中心”以完善授权撤回与查询功能，用户能够实时对“数据共享对象用途期限”进行查询，还能达成“一键撤回授权”操作。平台在撤回操作后要于 24 小时内停止数据共享行为，并把相关数据删除，需通过短信或者 APP 通知的形式向用户反馈处理结果，以此保证用户能够行使知情权与控制权。

对于用户支付信息，精准收货地址生物识别数据等敏感信息强化敏感数据的授权保护，需采用“双重验证授权”(如短信验证码 + 人脸识别)，而且每 6 个月重新获取用户授权。

(二) 把“清晰平台授权”当作权源根基，对权责边界予以界定

中国电子商务协会牵头制定标准化授权协议模板，并出台《电商平台第三方数据共享授权协议(示范文本)》，其中明确协议核心内容需涵盖“数据类型、使用范围、时间期限、禁止条款(禁止二次共享)、责任划分”等。可在模板中约定“第三方仅能于 XX 电商平台范围内使用用户数据，将其用于 2024 年 6~8 月期间的夏季服饰营销活动，绝对禁止把数据共享给任何第三方主体”以此减少兜底条款。

(三) 以“全流程管控”为实施保障，防范链条断裂

参考《信息安全技术个人信息匿名化指南》(GB/T35273-2020)明确数据脱敏的授权豁免标准，其中规定"有效匿名化"要满足"无法识别单个用户，无法复原无法关联其他数据"这三个要件。电商平台需将脱敏数据委托给第三方机构进行审计，只有在审计通过之后才能够豁免授权，需重新获取授权，若后续数据用途变更或再识别风险上升[11] [12]。

在原授权协议里明确规定“第三方不得将数据二次共享给任何主体，除非获得原平台与用户的双重同意”约定了“二次共享的违约责任”(支付违约金终止合作等)严禁第三方二次共享[9]。

6. 结论与建议

数据确权不是要扼杀网络营销的创新活力，而是通过划清权利边界，为其划定一条清晰、安全的赛道，推动企业从粗放利用转向精细使用，实现可持续发展。

(一) 结论

在网络营销第三方数据共享里“三重授权”原则所面临的适用困境，其本质是“法律原则性规定”同“电商实践复杂性”以及“商业效率需求”这三者间的矛盾。构建“有效用户授权－清晰平台授权－全流程管控”这样的合法边界体系，能够达成“个人信息保护、企业合规经营、电商营销创新”这三方的平衡。推动第三方数据共享营销从“粗放式”迈向“精细化”转型，既要保障用户对数据的控制权，又得为电商企业与第三方服务商给出明确的合规路径。

(二) 建议

电商平台在企业层面构建内部合规体系时，应设立“数据共享合规部门”，该部门负责对第三方合作方资质进行审查，对授权协议展开审核并对数据流转过程予以监控；在产品研发的起始阶段将“合规模块”嵌入其中(场景化授权功能，以及授权撤回功能等)达成“合规前置”的目标，将典型违法案例与“三重授权”操作标准作为重点内容，定期开展员工合规培训以此提升合规意识。

在监管层面加快出台《电商数据第三方共享管理办法》，以细化规则与强化执法，明确“用户授权有效性标准”“数据脱敏技术规范”“平台授权协议必备条款”；构建“电商数据共享监管平台”，运用大数据技术实时对数据流转情况予以监测，针对“伪授权”“超范围共享”之类行为自动发出预警提高监管效率。

从行业角度出发，电商行业协会应大力推动自律与协同，开展“数据共享合规认证”工作，针对合规达标的企业颁发认证证书，以此引导消费者优先选择合规平台；建立“行业合规数据库”，将典型案例合规模板以及文献资料进行汇总，以此为企业给予参考，推动行业整体合规水平提升，组织企业开展合规经验交流。

参考文献

[1] 艾瑞咨询. 2024 年中国电商营销数据共享行业研究报告[R]. 艾瑞咨询集团, 2024.

[2] 丁晓东. 个人信息保护: 原理与实践[M]. 北京: 法律出版社, 2021.

[3] 申卫星. 论数据用益权[J]. 中国社会科学, 2020(11): 123-140.

[4] 国家网信办. 电商数据安全管理指引(征求意见稿) [Z]. 2023.

[5] 潘煜萌. 电商平台中的个人信息保护研究[D]: [硕士学位论文]. 银川: 北方民族大学, 2025.

[6] 王丹, 姜艺, 陆伟. 数智时代信息服务中的隐私困境及应对策略——基于隐私让渡视角的探索[J]. 中国图书馆学报, 2024, 50(3): 67-81.

[7] 徐伟, 李文敏. 数智时代 App 收集个人信息的安全风险与法律应对[J]. 山东行政学院学报, 2025(1): 113-121.

[8] 张基利, 康兰平. 电商平台中公民个人信息保护的规范路径探讨——基于 APP 隐私政策的实证研究[J]. 现代商贸工业, 2022, 43(21): 181-183.

[9] 梁栋. 电子商务消费者个人信息保护的规范路径——基于 6 类 12 家电商平台隐私政策的实证研究[J]. 大连理工大学学报(社会科学版), 2022, 43(3): 102-112.

[10] 崔冠云, 王璞. 风险挑战与敏捷治理: 数字经济背景下的个人信息保护[J]. 图书馆论坛, 2024, 44(3): 88-95.

[11] 陈国军. 论大数据时代个人信息的私法保护与共享[J]. 河南师范大学学报(哲学社会科学版), 2022, 49(1): 66-73.

[12] 国家市场监督管理总局, 国家标准化管理委员会. GB/T 35273-2020 信息安全技术个人信息匿名化指南[S]. 2020.