E-Commerce Letters 电子商务评论, 2026, 15(5), 407-414
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2026.155533

Hans汉斯

电商精准广告投放中个人信息保护的路径研究

余　蓉

浙江理工大学法学与人文学院，浙江　杭州

收稿日期：2026年3月11日；录用日期：2026年3月23日；发布日期：2026年5月22日

摘　要

电商精准广告投放依托大数据与算法技术实现了营销效能，却也引发了个人信息非法收集、二次侵害等多重权益危机。我国《个人信息保护法》《数据安全法》等立法虽已构建基本的保护框架，但在电商司法实践中仍存在法律属性界定模糊、分级保护滞后、“告知－同意”机制形式化及第三方流转监管缺失等问题。本文立足最新立法实践，融合计算机科学、经济学分析视角并借鉴域外经验，提出构建“风险评估 + 类型化保护”的双重机制，通过完善电商“个性化协议”优化权利保障模式，落实“用者有其责”的全链条追责机制，并引入多元共治体系，力求实现电商的商业价值与个人信息权益保护的动态平衡，为数字经济时代个人信息保护的法学理论研究提供深化思路。

关键词

电商精准广告，个人信息保护，信息自决权

Research on Personal Information Protection in Targeted Advertising for E-Commerce

Rong Yu

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: March 11, 2026; accepted: March 23, 2026; published: May 22, 2026

Abstract

Precision advertising in e-commerce leverages big data and algorithmic technologies to enhance marketing effectiveness, yet it has also triggered multiple crises, such as illegal collection of personal information and secondary infringement. Although China’s “Personal Information Protection Law” and “Data Security Law” have established a basic protective framework, judicial practice in e-commerce

文章引用: 余蓉. 电商精准广告投放中个人信息保护的路径研究[J]. 电子商务评论, 2026, 15(5): 407-414.
DOI: 10.12677/ecl.2026.155533

still faces issues including ambiguous legal characterization, lagging tiered protection, formalistic "notice-and-consent" mechanisms, and inadequate oversight of third-party data transfers. This paper, grounded in recent legislative developments, integrating perspectives from computer science and economics and drawing on international experiences, proposes establishing a dual mechanism of "risk assessment + typified protection". It advocates refining e-commerce "personalized agreements" to optimize rights safeguarding models, implementing a full-chain accountability mechanism based on the principle of "responsibility lies with the user", and introducing a multi-stakeholder governance system. These measures aim to achieve a dynamic equilibrium between e-commerce's commercial value and the protection of personal information rights, thereby providing insights for further research into the legal theory of personal data protection in the digital economy era.

Keywords

E-Commerce Precision Advertising, Personal Information Protection, Right to Informational Self-Determination

1. 引言

(一) 研究背景

当下，人类社会已全面迈入数字化新纪元，呈现出“终端泛在化、万物互联化、网络全覆盖以及时刻在线化”的显著特征。人们每天在社交媒体(微博、微信等)上分享与自己相关的海量信息，表达自己个性化需求的同时，也有大量的信息(如网站浏览历史、行程轨迹位置，网购物品记录等)在信息主体没有参与甚至不知情的情况下，被互联网公司通过 Cookie 技术、用户画像构建算法等计算机技术储存、分析并整合着[1]。随着大数据技术与电商经济的深度融合，精准广告投放已成为商业营销的核心形态。相较于传统“广撒网”式营销，电商精准广告依托算法技术对用户个人信息的深度挖掘，生成个性化“数字档案”，实现“量体裁衣”式的营销转化。

但技术革新与电商利益的双重驱动，也加剧了个人信息保护的风险。一方面，电商精准广告投放高度依赖用户网络行为信息，而此类信息的法律属性界定不明，导致信息处理活动缺乏明确规范；另一方面，网络服务提供者与用户之间的信息控制能力失衡，部分主体为追求电商流量变现，存在过度收集、随意共享用户信息等不当行为，引发了隐私担忧与权益纠纷问题。从经济学视角看，此类行为本质上是信息不对称下的市场失灵，电商平台凭借信息优势降低自身营销成本，却将个人信息泄露的风险成本转嫁给消费者，长期来看将损害电商产业的市场信任与可持续发展。在此背景下，如何在保障电商经济创新发展的同时，构建有效的个人信息保护机制，寻求一条合理的破解平衡之道，成为当前亟待解决的法律与社会问题。

(二) 研究意义

理论上，本文立足民商法学视角，融合计算机科学、经济学跨学科分析方法，结合实证分析与比较研究方法，厘清电商精准广告投放中个人信息的法律属性与保护边界，借鉴域外“三分法”信息分级标准，弥补现有研究中技术机制与法律规制结合不足的缺陷，丰富电商经济时代个人信息保护的理论体系。实践中，通过剖析电商精准广告投放中的个人信息保护困境，借鉴域外成熟经验，提出具有可操作性的具体规制方案，可为立法机关修订相关法律法规、监管部门强化电商行业监管、网络服务提供者规范信息处理行为提供参考，助力实现电商行业创新与个人信息保护的良性平衡。

(三) 研究思路与内容

本文以电商精准广告投放中的个人信息保护为核心研究对象，遵循“机制剖析－困境梳理－经验借鉴－路径完善”的逻辑展开。首先，结合计算机科学技术特征解析电商场景下精准广告投放中个人信息的界定标准与类型划分；其次，结合最新电商案例梳理当前我国个人信息保护面临的立法与实践难题；再次，通过比较欧盟与美国的相关立法与司法实践，提炼可借鉴的经验；最后，结合我国本土电商经济实际，从法律界定、分级标准、权益保障及侵权救济四个维度提出完善建议与操作方案，重点明确“风险评估 + 类型化保护”“三分法”分级保护等核心机制的实施路径。

2. 精准广告投放中个人信息的界定与保护基础

(一) 个人信息类型与法律属性

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。而在电商经济中，精准广告投放的核心技术支撑是Cookie机制及电商平台内部追踪代码，其通过追踪用户网络行为、收集相关信息构建用户画像，为个性化推送提供数据基础[2]。Cookie机制收集的个人信息主要包括两类：一是用户基本身份信息，涵盖姓名、性别、年龄、身份证号码、联系方式、财产状况等，此类信息具有直接识别性，普遍被纳入个人信息范畴；二是网络行为信息，包括IP地址、设备序列号、浏览记录、搜索历史、电商交易数据等，此类信息的法律属性存在较大争议，是电商精准广告个人信息保护的核心焦点。

学界对网络行为信息的法律属性存在多元观点：“个人信息说”认为，尽管网络行为信息多为碎片化数据，但经技术整合后可间接识别特定自然人，应将其归入个人信息范畴[3]；“隐私说”主张，网络行为信息反映用户兴趣偏好与生活轨迹，属于个人不愿公开的私密信息，应受隐私权保护[4]；“网络碎片信息说”与“计算机数据说”则认为，此类信息仅为与终端设备相关的技术数据，无法关联特定自然人，不应被界定为个人信息[5]。

笔者认为，在电商经济蓬勃发展的背景下，网络行为信息的法律属性不应一概而论，而是结合其技术层面的可识别性与法律层面的关联性特征综合判断。在大数据技术迭代升级的背景下，碎片化的网络行为信息通过算法整合可重构完整的用户画像，具备间接识别特定自然人的能力，符合个人信息的核心特征。鉴于此，亟需在立法层面确立网络行为信息的个人信息这一法律地位，从而为电商经济环境下的权利配置与救济机制夯实规范基础。

(二) 个人信息保护的核心原则

根据《个人信息保护法》，对个人信息的处理需遵循三大核心原则：一是合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息，确保数据处理活动始终在法治轨道上运行，从经济学角度来看，该原则的本质是划定电商平台信息处理的市场行为边界，防止平台利用信息优势实施不正当竞争；二是最小必要与限于目的原则，严格限定信息收集的范围与频率，不得过度收集信息且信息的收集应采取对个人权益影响最小的方式；三是公开、透明原则，要求公开个人信息处理规则，明示处理的目的、方式和范围。

3. 我国精准广告投放中个人信息保护的现实困境

(一) 网络行为信息性质界定模糊

1) 立法界定存在模糊性

我国现行法律体系中尚未对电商网络行为信息的性质作出清晰界定。仅国家标准化管理委员会发布的《信息安全技术－个人信息安全规范》(下文简称《信息安全规范》)中以不完全列举的方式，将网站浏览记录、电商购物记录等个人网络行为信息归类于个人信息的范畴，但该规范缺乏法律层面的强制约束力，难以直接作为执法依据。此外，《个人信息保护法》规定匿名化处理后的信息不属于个人信息，却未

细化“无法识别”“不能复原”的具体认定标准，这一立法空白导致实践中电商平台常借“匿名化”之名行免责之实，而技术发展已使匿名化信息存在重新识别的可能，导致法律保护出现漏洞。

2) 司法裁判标准不一

司法实践中，法院对电商网络行为信息的性质判定差异显著。以“朱烨诉百度案”为例[1]，一审法院认定网络行为信息属于个人隐私，而二审法院则主张经匿名化处理后因无法确定信息归属主体，该类信息不属于个人信息。与之相反，“陈某诉杭州某软件服务公司案”[2]的判决中明确指出，网络行为信息可单独或结合其他信息识别特定自然人，应认定为个人信息。此类同案不同判的现象的司法分歧来源于立法界定模糊，加剧了电商经济环境下个人信息保护的不确定性。

(二) 信息分级处理面临复杂挑战

我国《个人信息保护法》采用“敏感信息–一般信息”的二元分级模式，将生物识别、医疗健康、金融账户等信息列为敏感个人信息，规定了特殊处理规则，其他信息作为一般信息则适用普通规则[6]。然而，面对电商精准广告投放的复杂场景，该二元架构显现出明显的局限性：

1) 分级标准过于宏观，覆盖范围不全

在电商广告定向投放过程中，用户碎片信息虽然单独不构成敏感信息，但经算法整合后可形成具有高度敏感性的行踪轨迹或消费画像，现行的二元分级模式难以有效规制此类“量变引起质变”的数据衍生风险，导致保护链条出现断裂。例如，单一的浏览记录可能不敏感，但结合电商购买记录形成的画像则极具敏感性。

2) “捆绑式”收集现象普遍，分级保护流于形式

部分电商平台背离最小必要原则，以变相强制手段收集超出核心业务范畴的非必要个人信息，且往往未设置“拒绝”或“跳过”选项，这种“一揽子”授权模式使得事前分级筛选失去操作基础。例如部分电商 App 强制收集用户地理位置、社交关系等与核心功能无关的信息，直接造成信息分级处理无法落实其实际效能，阻碍了电商经济的健康有序发展。

(三) 用户个人信息权益面临多重侵害风险

1) 知情同意权的实效性困境

尽管“告知–同意”是个人信息处理的核心原则，但实践中存在形式化倾向。一方面，电商平台隐私政策文本呈现出冗长性与高专业度特征，其平均字数超 1.6 万字且充斥着晦涩的专业术语，使得普通用户难以实现有效认知，实证数据显示，绝大多数用户安装电商 App 时“很少或从未”阅读隐私协议；另一方面，部分网络服务提供者未以显著方式履行告知义务，甚至通过“默认勾选”“捆绑授权”等技术设计手段变相剥夺用户的自主选择权，致使知情同意规则流于形式。

2) 个人信息面临过度挖掘与共享双重风险

电商平台通过整合碎片化信息构建“用户数据仓库”，利用用户画像算法、行为预测模型等技术手段过度挖掘用户的兴趣偏好、行为轨迹等隐私信息，形成具有高度识别性的“整合性隐私”，以实现对用户的全面监控与精准操控。与此同时，在第三方广告商介入的投放模式中，信息跨平台共享现象普遍，部分电商平台未依法公开第三方共享清单，甚至违规转售用户信息牟利。例如“世纪佳缘”App 曾因私自向第三方共享用户信息遭工信部通报，这暴露出当前电商数据共享环节监管缺失的严峻性。

3) 个人信息泄露隐患日益严峻

Cookie 机制可存储长达 180 天以上的用户信息，电商平台通过服务器数据存储、云端数据同步等技

[1]见(2013)鼓民初字第 3031 号判决书，南京鼓楼区人民法院审理“朱烨诉北京百度网讯科技有限公司隐私权纠纷案”。
[2]见(2021)鄂 11 民终 3136 号判决书，湖北省黄冈市中级人民法院审理“陈婷、北京百度网讯科技有限公司个人信息保护纠纷案”。

术手段，能够实现对用户网络轨迹及私密信息的全时空记录，一旦安全防护措施不到位，大规模信息泄露事故便极易发生。既往案例表明，此类风险易造成严重后果：Facebook 曾发生超 5000 万用户数据泄露事件[3]，国内大型电商集团华住集团旗下酒店亦发生过 5 亿条客户信息被打包出售[4]。上述安全事件所涉数据多源于精准广告投放中的采集行为，不仅暴露了数据生命周期管理的薄弱环节，更对用户合法权益造成了实质性损害，从经济学角度看，此类事件也导致了电商行业的整体信任成本上升，不利于数字经济发展。

4. 精准广告个人信息保护的域外经验借鉴

(一) 欧盟：统一立法与区别保护模式

欧盟通过完善的立法与严格的执法，构建了全面的个人信息保护体系，为电商经济提供了清晰的合规指引。在网络行为信息界定方面，欧盟《数据保护指令》(DPD)、《隐私和电子通信指令》(EPD)及《通用数据保护条例》(GDPR)均明确将网络行为信息纳入个人信息范畴，强调其“可识别性”特征。GDPR 进一步在序言与正文中明确，在线标识等网络行为信息可与特定自然人关联，应受法律保护。

在司法实践中，欧盟法院通过判例强化网络行为信息保护。例如在 Patrick Breyer 诉德意志联邦共和国一案中，欧盟法院认为网络服务提供者将用户动态 IP 与其持有的其他用户信息相结合从而识别来访者身份是完全“合理且可能”的，故此类动态 IP 应当被视为个人信息，应当为其提供无间隙保护。

此外，欧盟要求网络服务提供者严格履行“告知–同意”义务，GDPR 规定个人同意必须是充分知情、自愿明确的意思表示，禁止默认同意或捆绑授权，并要求平台采用“清晰易懂的语言 + 可视化展示”的技术方式履行告知义务，降低用户的信息认知成本。与此同时，设立数据保护官(DPO)制度强化内部合规监督，并辅以高额行政处罚作为威慑，例如针对违规收集浏览记录用于广告画像的行为处以亿欧元级罚款，彰显了严格监管的力度，有力保障了电商经济中的用户权益。

(二) 美国：分散立法与行业自律结合模式

与欧盟不同的是，当前美国并没有统一的综合性个人信息保护法律，其采用“联邦立法 + 州立法 + 行业自律”的多元保护模式，以适应其活跃的电商经济。在立法层面，加利福尼亚州在 2018 年出台的《加州消费者隐私法》(CCPA)明确将浏览历史、搜索内容等网络行为信息纳入个人信息范畴，以立法的形式充分肯定了网络行为信息的可识别性；联邦层面的《美国数据隐私和保护法案》(ADPPA)草案也将网络行为信息列为受保护的个人信息。

在监管机制上，美国国家标准和技术研究所(NIST)选择以“泄露结果的严重程度”为准绳，按照个人信息在发生泄露的情况下可能造成的破坏程度将其划分为高、中、低三个级别，针对不同级别采取差异化保护措施。同时，美国通过行业自律机制补充立法不足，例如互联网企业推出“Do Not Track”功能，允许用户拒绝 Cookie 追踪，联邦贸易委员会(FTC)要求网络服务提供者为用户提供便捷的选择权。尽管“Do Not Track”机制因广告行业反对存在执行困境，但其核心思路为我国电商经济下的个人信息保护提供了借鉴。

(三) 域外经验的启示

结合欧盟与美国的实践经验，可提炼出三点启示：一是明确网络行为信息的个人信息属性，以此为电商个人信息保护提供法律基础；二是建立多维度信息分级标准，依据信息的可识别性、敏感程度及潜

[3]毛雅谊：《“脸书”泄露 5000 万用户数据用于什么目的？真相令人震惊》，载央视网 https://news.cctv.com/2018/03/22/ARTIgZtCK89eDZcUpNFJdw1Y180322.shtml，最后访问日期：2026 年 3 月 6 日。
[4]罗亦丹：《华住 5 亿条用户信息疑泄露 警方已介入调查》，载新京报 https://baijiahao.baidu.com/s?id=1610068769264753849&wfr=spider&for=pc，最后访问日期：2026 年 3 月 6 日。

在泄露风险采取差异化保护措施；三是强化“告知–同意”原则的落实，充分保障用户对个人信息的知情权与自主控制权，进一步健全个人参与保障体系，促进电商经济的可持续发展。

5. 我国精准广告投放中个人信息保护的完善建议

(一) 明确网络行为信息的个人信息属性

1) 立法层面予以界定

借鉴欧盟 GDPR 与美国 CCPA 的经验，通过推动《个人信息保护法》的修订进程或出台与之配套的司法解释，以明确列举的方式将 IP 地址、浏览记录、搜索历史、电商设备序列号等网络行为信息正式纳入个人信息范畴，明确其“可识别性”特征，消除立法模糊性[7]。同时，细化匿名化处理的认定标准，明确“无法识别”“不可复原”的技术要求与审查机制，防范电商平台以“匿名化”为由规避责任。

2) 司法层面统一裁判标准

通过发布指导性案例、出台司法解释等举措，统一司法机关对电商网络行为信息性质的认定标准，清晰划定其与个人信息、隐私权之间的界限，避免司法裁判过程中出现分歧。在审理此类相关案件时，法院应结合当下电商技术发展现状，认定网络行为信息经整合后是否具有识别特定自然人的功能，以此作为判断其是否归属于个人信息范畴的重要依据。

(二) 构建“三分法”信息分级处理标准

鉴于二元分级模式的局限性，建议确立“高度私密信息–一般私密信息–其他个人信息”的三级分层治理范式，并根据信息对用户的识别程度及与人格利益的关联程度，实施差异化保护策略，构建“风险评估–分级认定–动态调整”的全流程操作体系，以适应电商经济的复杂需求：

1) 高度私密信息：包括医疗健康信息、金融账户信息、生物识别信息、电商详细交易记录等，此类信息具有极高的个体指向性，与人格尊严、人身财产安全密切相关，应当适用最严格的保护规则。电商平台需单独告知信息处理目的、风险及保障措施，获得用户明示单独同意，同时采用加密存储等安全措施，定期向用户通报处理情况，并保障用户享有随时撤销授权的自由。

2) 一般私密信息：包括电话号码、IP 地址、工作单位等，此类信息具有一定隐私属性，但其识别程度与权益关联度相对有限。处理此类信息时，电商平台需清晰阐释处理规范，不得采用“一揽子”授权或默认同意模式，必须确保获得用户的明确同意，定期提醒用户行使其撤回权。

3) 其他个人信息：包括姓名、性别、年龄、浏览记录、搜索历史等，此类信息识别性较弱，与核心人格利益关联不紧密，是电商精准广告投放的基础数据。对其管理应遵守《个人信息保护法》的一般规定，在保障用户的知情权与撤回同意权的基础上，可探索“白名单”机制实现批量同意，提高电商信息处理效率。

4) “三分法”分级保护的全流程操作体系

由电商平台建立内部风险评估小组，由法律、技术、运营等部门人员组成，定期对平台收集的个人信息进行风险评估，结合技术特征与经济影响，判断信息的分级类型，评估报告需向网信部门备案；网信部门建立电商个人信息分级认定平台，接受电商平台的分级认定申请，对高度私密信息的分级进行实质审查，对一般私密信息与其他个人信息进行形式审查，审查通过后发放分级认定标识；结合技术发展与电商产业变化，网信部门修订该规则实施指南，电商平台需根据指南更新及时调整信息分级与保护措施，若信息的风险程度发生变化，需在规定时间内重新进行风险评估并向网信部门报备。

(三) 强化个人信息权益保障机制

1) 优化“告知–同意”机制

在形式方面，电商平台应简化隐私政策内容，采用清晰易懂的语言与可视化形式呈现核心信息，制

作要点摘录置于隐私政策首页，降低用户阅读门槛；在语言风格方面，严格规避模糊性表述及艰深晦涩的专业术语，避免采用浅灰色字体、隐藏文本等方式规避告知责任；在告知内容方面，区分不同级别信息的同意方式，禁止默认勾选、捆绑授权等行为，确保用户在充分知悉信息处理风险的基础上，作出真实、自愿且明确的意愿表示。

2) 完善“Do Not Track”机制

建议将“Do Not Track”功能纳入法定权利，要求电商浏览器于 App 中设置便捷的“一键关闭”选项，用户开启该功能后，不得再追踪其网络行为或收集相关信息[8]。同时应建立行业监管机制，对未落实“Do Not Track”功能的电商企业予以处罚，保障用户的自主选择权。

3) 细化个人参与规则

明确用户查阅、复制、更正、删除个人信息的权利行使路径，首先要求在电商平台内设置专门功能模块，支持用户在线便捷调取网络行为信息等数据。其次，规定信息处理者的响应期限，对用户的更正、删除请求，应在合理期限内完成处理并反馈处理结果。最后，赋予用户算法解释权，要求电商平台对精准广告的推送逻辑、数据来源进行说明，确保用户在自动化决策过程中的知情权与监督权得以实质落地。

(四) 明确侵权救济方案

1) 网络服务提供者侵权的救济

电商平台违反“告知–同意”原则，过度收集、不当处理个人信息的，用户有权主张停止收集、存储并删除相关信息；若造成实质性损害，用户可依据《民法典》《个人信息保护法》的相关条款提起损害赔偿诉讼，赔偿数额可根据用户的实际损失或电商平台的违法所得予以确定。

2) 广告商侵权的救济

可借鉴《产品质量法》《消费者权益保护法》的相关规定，赋予用户向广告商主张权利的路径。广告商负有向用户披露电商平台联络信息的法定义务，并协助用户核实侵权事实；若广告商无法提供相关信息或存在过错的，应与电商平台承担连带赔偿责任。

3) 第三方侵权的救济

若电商平台与广告商未履行安全保障义务，导致用户信息遭受第三方窃取、泄露或篡改的，应在其过错范围内承担补充赔偿责任。针对擅自获取、利用用户信息的第三方主体，用户不仅可要求其停止侵害并赔偿损失；对于情节严重、触犯刑法的行为，还应依法启动刑事追责程序，构建民事赔偿与刑事制裁相结合的多维救济体系，护航电商经济安全。

6. 结语

精准广告投放作为电商经济时代的商业引擎，在重塑营销范式的同时，也引发了个人信息权益与数据商业价值之间的冲突。本文通过对我国现行立法框架的审视与司法实践困境的剖析，揭示了当前保护机制中存在的核心症结：网络行为信息的法律属性导致确权苦难，“敏感–一般”二元分级模式难以应对碎片化数据聚合带来的衍生风险，“告知–同意”机制的形式化削弱了用户的实质控制权，以及全链条追责体系的缺位致使侵权成本过低。

针对上述问题，本文立足于本土法治并借鉴域外成熟经验，提炼出一套系统性的治理路径。首先，必须在立法与司法层面明确网络行为信息的“个人信息”属性，夯实权利保护的逻辑起点；其次，突破传统二级架构，构建“三分法”的分级处理标准，致力于实现从“一刀切”到“差异化”的精准规制；再次，通过重构可视化告知流程、法定化“DNT”机制及细化算法解释权，推动用户权益保障从被动防御转向主动控制；最后，确保包含电商平台、广告商及第三方在内的全链条侵权责任体系，特别是引入连带责任与补充责任机制，以严密的法网倒逼行业合规。

展望未来，个人信息保护并非要扼杀技术创新或阻碍电商经济发展，而是旨在通过规则的完善，为数据要素的流动划定清晰的边界。唯有在法治轨道上实现技术理性与人文关怀的有机统一，构建起政府监管、行业自律与社会共治相结合的多元治理格局，方能真正破解电商精准广告领域的“隐私悖论”，做到真正尊重和保障用户的个人信息权益，为电商经济的可持续发展奠定坚实基础。

参考文献

[1] 李媛. 大数据时代个人信息保护研究[M]. 武汉: 华中科技大学出版社, 2019.

[2] 宁宣凤, 吴涵, 黄若. Cookie 与个人信息保护[C]//《上海法学研究》集刊(2020 年第 13 卷 总第 37 卷)——金杜律师事务所、金杜研究院文集. 上海: 上海人民出版社, 2020: 162-167.

[3] 高富平. 基于规范目的的个人信息治理规则[J]. 中国应用法学, 2022(6): 111-127.

[4] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.

[5] 涂燕辉. “上网轨迹”信息的法律界定及其商业化利用界限——以朱烨诉百度 Cookie 侵权案为例[J]. 北京政法职业学院学报, 2016(3): 47-53.

[6] 裴俊晖, 刘柳. 区分于隐私的个人信息分级保护研究[J]. 社会科学动态, 2024(1): 87-94.

[7] 钟玉清. 论电子商务领域个人信息保护的完善[J]. 时代人物, 2022(34): 246-248.

[8] 李兴鹏. 跨境电商中个人信息保护的制度构建与完善——评《跨境电子商务法律问题研究》[J]. 科技管理研究, 2022, 42(7): 244.