E-Commerce Letters 电子商务评论, 2025, 14(9), 1718-1725
Published Online September 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1493097

Hans汉斯

数据库营销的隐私权边界与合规路径

王　涛

贵州大学法学院，贵州　贵阳

收稿日期：2025年7月28日；录用日期：2025年8月7日；发布日期：2025年9月19日

摘　要

数据库营销凭借数据技术实现精准化运营，成为数字经济时代的重要营销范式，但也让隐私权保护与数据价值利用的矛盾日益凸显。本文围绕数据库营销中隐私权边界的动态界定与合规路径展开研究，解析了隐私权边界在理论上的争议(控制说、合理预期说、风险预防说)和立法层面的模糊性，揭示了司法实践中“场景依赖”的裁判逻辑。通过场景化分析数据收集、处理、共享、触达全流程的隐私风险，指出用户敏感度、企业透明度、技术脱敏水平是影响边界感知的关键因素。对比欧盟、美国、日韩及我国的合规实践，剖析了过度采集、默认同意陷阱、跨境传输违规等典型问题及根源，最终提出多维度合规路径：法律层面细化场景化规则与完善权利救济，企业层面构建“数据治理－用户权利－技术保障”体系，行业与社会层面强化自律与监督协同。研究为平衡数据商业价值与隐私保护提供了理论框架与实践指引，助力数据库营销的合规化与可持续发展。

关键词

数据库营销，隐私权边界，合规路径，数据保护，场景化治理

Privacy Boundaries and Compliance Paths in Database Marketing

Tao Wang

School of Law, Guizhou University, Guiyang Guizhou

Received: Jul. 28th, 2025; accepted: Aug. 7th, 2025; published: Sep. 19th, 2025

Abstract

Database marketing, leveraging data technologies to achieve precise operations, has become a crucial marketing paradigm in the digital economy era. However, it has increasingly highlighted the contradiction between privacy protection and the utilization of data value. This paper focuses on the dynamic definition of privacy boundaries and compliance paths in database marketing, analyzing

文章引用: 王涛. 数据库营销的隐私权边界与合规路径[J]. 电子商务评论, 2025, 14(9): 1718-1725.
DOI: 10.12677/ecl.2025.1493097

theoretical controversies over privacy boundaries (including the control theory, reasonable expectation theory, and risk prevention theory) as well as legislative ambiguities. It also reveals the "context-dependent" judicial logic in judicial practice. Through a scenario-based analysis of privacy risks throughout the entire process of data collection, processing, sharing, and outreach, the paper identifies user sensitivity, corporate transparency, and technical desensitization levels as key factors influencing the perception of boundaries. By comparing compliance practices in the European Union, the United States, Japan, South Korea, and China, it examines typical issues such as excessive data collection, default consent traps, and cross-border transmission violations, along with their root causes. Finally, it proposes multi-dimensional compliance paths: refining scenario-specific rules and improving rights remedies at the legal level; building a "data governance-user rights-technical guarantee" system at the corporate level; and strengthening self-regulation and supervisory collaboration at the industry and social levels. This research provides a theoretical framework and practical guidance for balancing the commercial value of data and privacy protection, facilitating the compliance and sustainable development of database marketing.

Keywords

Database Marketing, Privacy Boundaries, Compliance Paths, Data Protection, Scenario-Based Governance

1. 引言

在数字化浪潮驱动下，数据库营销凭借精准用户画像与个性化推荐能力，已成为企业提升市场竞争力的核心手段。大数据技术更推动其从传统“广撒网”模式转向精准化范式——企业通过构建数据库，整合用户描述信息(如年龄、职业)、行为信息(如消费记录、浏览轨迹)及关联信息(如偏好与忠诚度)，实现目标客户精准定位，典型如 Facebook 通过“点赞”数据预测用户特征、阿里巴巴依托海量消费数据优化推荐，显著降低营销成本并提升投资回报率，成为数字经济时代企业核心竞争力的重要来源。

然而，数据挖掘技术深化与营销规模扩张，也使商业效率与隐私权保护的冲突日益尖锐：企业通过 Cookie 追踪、设备指纹等技术被动获取隐性信息，或在注册环节收集显性信息，形成“全景监控”；过度采集(如强制授权冗余权限)、知情同意机制虚化(如晦涩隐私条款)、数据滥用(如未授权转售第三方)及二次交易频发，不仅导致信息泄露事件(如社交平台数据出境被罚、快递信息用于营销侵权)，更持续侵蚀用户数据控制权与人格尊严。本质上，这是企业数据价值最大化诉求与用户隐私权保障需求的博弈，因此厘清隐私权合理边界、探索可持续合规路径，兼具理论必要性与现实紧迫性。

2. 数据库营销中隐私权边界的界定困境与场景化分析

2.1. 隐私权边界的理论争议与立法模糊性

隐私权边界的理论界定始终随着数字技术的发展而动态演变，学界对此存在显著争议。传统“独处权”理论由沃伦与布兰代斯提出，强调私人空间不受侵扰，但在数据库营销场景中已难以覆盖数据维度的隐私需求，王利明在其研究中也指出，隐私权的内涵需向“生活安宁”与“私人秘密”拓展[1]。当前核心争议聚焦于三大观点：“控制说”认为隐私权的核心是个人对数据收集、使用、传播的控制权，例如用户有权决定是否允许企业通过 Cookie 追踪其浏览行为，但这一理论难以平衡“数据最小化”与“营销

效率”的冲突，企业为精准定位需多维度数据，而用户完全控制可能导致数据维度不足，削弱营销价值；“合理预期说”以用户对隐私的合理期待为边界，例如用户通常预期购物记录用于推荐而非转售，但数据库营销中，算法对碎片化数据的聚合常超出用户预期，而且合理预期的标准也难以量化；“风险预防说”主张以数据滥用的潜在风险划定边界，如生物识别信息因泄露风险高应严格限制，但过度强调风险会抑制数据价值释放，例如金融企业若无法利用用户信用数据，精准营销将无从谈起。这些理论分歧本质上反映了“个人权利保护”与“数据商业价值”的张力，而数据库营销的技术复杂性(如跨平台数据整合)进一步加剧了界定难度[2]。

立法层面，当前主流框架虽确立了隐私保护原则，但具体适用存在显著模糊性。我国《个人信息保护法》与欧盟 GDPR 均将“合法、正当、必要”作为核心原则，但“必要范围”缺乏明确标准，例如电商平台收集用户地理位置信息，究竟是为配送服务(必要)还是精准广告投放(非必要)，企业与用户常存在认知分歧。匿名化与个人信息的边界同样模糊，立法要求匿名化数据不受隐私权约束，但数据库营销中“去标识化数据”易被重新识别。此外，跨境数据传输存在规则冲突，GDPR 要求向第三国传输数据需满足“充分保护”标准，而我国采用“安全评估 + 白名单”模式，跨国企业为实现全球数据库联动，常陷入“合规即失效”的困境。

司法实践中，隐私权边界的判定呈现“场景依赖”特征，不同场景下的裁判逻辑差异显著。国内“快递信息用于营销”侵权案中，某快递公司将用户姓名、电话、地址等信息出售给电商平台用于定向营销，法院认定构成侵权[1]，核心在于“数据用途超出收集时的明示范围”，强调“目的特定性”原则；欧盟“谷歌数据聚合”案中，谷歌将用户搜索记录、地图定位等数据整合用于个性化推荐，欧盟法院判定其违反 GDPR，理由是“未获得用户针对数据聚合的单独同意”，凸显“数据关联性”对隐私边界的影响；美国“Facebook 定向广告”争议中，Facebook 通过分析用户社交关系链推送广告，法院未认定侵权，因美国采用“行业自律 + 事后救济”模式，更侧重市场调节。这些案例表明，隐私权边界的司法判定与立法理念深度绑定，欧盟侧重“权利优先”，我国强调“目的限制”，美国依赖“市场自治”，这种差异进一步加剧了企业的合规难度[3]。

2.2. 数据库营销全流程的隐私边界场景化解构

数据库营销的“数据收集–处理–共享–触达”全流程中，隐私权边界因技术手段、数据类型、应用场景的不同而动态变化，需进行场景化拆解。在数据收集阶段，主动提供与被动获取的信息存在显著边界差异。用户通过注册、问卷等方式主动提交的信息(如姓名、电话、消费偏好)，其隐私边界相对清晰，企业需明确告知用途，且不得超出范围使用。例如用户在电商平台注册时提供的收货地址，若被用于配送以外的营销(如短信推销)，即突破边界。而通过 Cookie、设备指纹、浏览轨迹等技术被动收集的数据，其边界模糊性显著，此类数据虽匿名，但结合 IP 地址、时间戳等可识别个人，应纳入隐私保护范围，实践中，浏览器厂商通过“隐私模式”为用户提供选择权(如 Chrome 的“无痕浏览”)，但企业常以“优化体验”为由默认开启追踪，导致边界被隐性侵蚀[4]。

数据处理阶段的核心争议是“匿名化处理后的数据是否仍受隐私保护”。企业常通过删除姓名、身份证号等直接标识符实现“伪匿名化”，但保留性别、年龄、消费习惯等间接标识符，第三方可结合社区公开信息锁定具体用户，因此“伪匿名化”数据仍具有隐私属性，但其边界难以通过技术手段固定。同时，数据挖掘算法(如协同过滤、聚类分析)的不透明性，使得用户无法知晓自身数据被如何处理，例如用户收到与疾病相关的定向广告，却不知晓算法如何通过其浏览记录推断健康状况，这种“算法歧视”本质上是对隐私自主决定权的侵犯。

[1] https://www.chinacourt.cn/article/detail/2024/11/id/8190923.shtml.

数据共享阶段，企业与第三方(如数据代理商、广告平台)共享数据时，“二次授权”成为边界判定的关键。若用户同意“数据仅用于本企业营销”，则企业向第三方共享需再次获得同意，符合《个人信息保护法》第 23 条规定。而多个企业共建“数据池”共享用户数据(如零售、支付、社交平台联合建模)时，即使单个企业的数据不敏感，聚合后可能触及隐私边界，此类模式因责任划分模糊，易成为隐私泄露的重灾区。营销触达阶段的边界集中于“用户接受度”与“推送合理性”。同一用户短时间内收到大量同类广告(如一天内 10 条贷款推销短信)，即使内容相关也可能构成骚扰，消费者对过度营销也有抵触情绪；而基于用户近期搜索记录的低频率推荐(如搜索“旅游”后收到 1 条酒店广告)，通常被视为合理边界内，此类精准推送的营销价值应当认可。此外，企业以“用户未拒绝”为由默认其接受营销(如 APP 隐私政策中隐藏“同意接收广告”条款)，此类“沉默同意”被司法实践否定，“明示同意”对边界界定具有必要性[5]。

3. 数据库营销的合规现状与挑战：基于国内外实践的比较

3.1. 国际合规框架与企业实践

全球数据库营销合规呈现多元路径，欧盟、美国及日韩的模式最具代表性。欧盟将隐私视为基本人权，以立法构建严格管控体系，1995 年《欧盟个人数据保护指令》及后续 GDPR 确立“数据最小化”、“目的限制”原则，要求企业收集数据需有合法目的且不超初始范围，还赋予用户被遗忘权等权利[6]。企业实践中，亚马逊为符合 GDPR 建立数据自动清理机制，定期删除超期浏览记录，并通过隐私影响评估工具审核数据使用合法性。美国采用“行业自律为主、立法补充”模式，联邦层面无统一法典，通过分散立法规范特定领域，如《儿童在线隐私保护法案》限制未成年人信息收集；行业协会如网络广告局推出自律计划，要求企业明确数据规则并提供退出渠道。Facebook 的广告定向实践体现了这一模式，其通过“隐私设置中心”让用户自主选择，但 2018 年剑桥分析事件暴露了自律模式的风险。日韩兼顾本土特点，日本 1982 年《个人数据信息处理中隐私保护对策》提出“限制收集”“正确管理”原则，2003 年《个人信息保护法》引入“匿名加工信息”制度，允许匿名化数据用于营销分析；韩国《个人信息保护法》要求数据共享需用户“单独同意”，并设专门机构监管，在金融、电商领域效果显著。

3.2. 我国数据库营销的合规现状与典型问题

我国数据库营销的合规框架以《个人信息保护法》为核心，辅以《电子商务法》《数据安全法》等形成体系，确立了“合法、正当、必要”“知情同意”等基本原则。《个人信息保护法》第 28 条特别强调，处理敏感个人信息(如生物识别、金融账户信息)用于营销时，必须获得用户“单独同意”，且需明确告知使用范围；第 44 条赋予用户“撤回同意”的权利，要求企业提供便捷的撤回渠道。这些规定为数据库营销划定了基本边界，例如电商平台若想使用用户的医疗健康数据推送保健品广告，必须单独获得用户授权，且用户可随时取消授权[7]。

但实践中，行业仍存在诸多合规乱象。一是过度采集非必要信息，部分企业为扩大营销数据维度，在用户注册时强制要求提供与服务无关的信息，如健身 APP 索要用户的房产信息、社交软件收集用户的通讯录细节，这种“数据囤积”行为违反了必要原则。二是默认同意陷阱普遍存在，企业常将“同意接收营销信息”设为注册默认选项，用户若不主动取消则视为授权，例如某外卖平台在用户下单时默认勾选“同意接收商家优惠短信”，导致用户频繁收到无关推送。三是数据跨境传输违规，部分跨国企业为实现全球营销数据联动，未经安全评估将中国用户数据传输至境外服务器，2023 年某社交平台因违规向境外传输用户画像数据被处罚 [2]，暴露了跨境合规的薄弱环节。

[2]http://www.legaldaily.com.cn/international/content/2023-05/29/content_8858982.html.

企业在合规实践中还面临多重困境。中小企业受制于技术与资金，难以建立完善的数据治理体系，例如缺乏加密技术导致用户数据存储安全系数低，或无力开发隐私设置功能满足“撤回同意”要求，谢贵荣指出，国内多数中小企业的数据库仅能实现基础存储功能，难以应对合规要求[8]。大型企业则面临“合规成本与营销效率”的矛盾，某头部电商平台数据显示，为符合“单独同意”要求，其用户授权率下降 15% [9]，导致精准营销的转化率降低，而引入隐私计算技术(如联邦学习)的研发成本又大幅增加，这种“合规即降效”的困境制约了数据库营销的健康发展。

3.3. 合规挑战的根源分析

合规困境源于技术迭代、监管协同与权利救济机制的交织问题。技术层面，大数据与 AI 发展远超立法更新，传统规则难覆盖新兴场景。如联邦学习“数据可用不可见”模式模糊“收集”与“使用”边界，现有法律对授权及责任界定不明；设备指纹技术通过设备特征识别用户，隐蔽性使知情同意形同虚设监管协同不足加剧执行碎片化，我国涉及网信、市场监管、工信等多部门，权责交叉导致企业重复检查，而跨平台数据共享等灰色地带存在监管空白。国内缺乏统一行业标准，不同地区对“必要原则”解释差异，增加企业跨区域合规成本。用户权利救济机制不畅削弱约束力，维权面临“举证难、赔偿低”问题。用户需证明企业违规及自身损失，但企业掌握数据优势，举证困难；即使胜诉，赔偿金额低，难形成震慑。集体诉讼制度不完善，分散用户难以抗衡企业，部分企业存“违法成本低于合规成本”的侥幸心理。这些问题凸显构建“技术–法律–行业”协同治理体系的迫切性，唯有让技术服务合规、规则适应技术、自律补充监管，才能平衡数据利用与隐私保护。

4. 数据库营销的多维度合规路径构建

4.1. 法律规制的完善：从原则性框架到场景化细则

法律作为合规路径的基础，需在现有原则框架下细化适用规则，兼顾数据利用与隐私保护的动态平衡。王利明中指出，隐私权作为具体人格权需依托明确法律边界[1]，这一思路可延伸至数据库营销立法完善中。针对“合法、正当、必要”原则的场景化落地，可通过“数据敏感度–处理目的–行业属性”的维度组合明确“必要”边界，例如电商平台为交易核心目的收集用户中敏级的收货地址、手机号符合要求，若为精准广告推送强制收集极高敏的人脸识别信息则超出边界；金融机构为风控可收集高敏的征信记录，却不可为理财产品推荐收集极高敏的病历信息，企业需在数据收集前提交相关匹配说明作为合规审查依据。

对于算法应用规范，需将王菲提及的算法备案细化为“清单式备案 + 动态评审”机制。企业需向网信部门提交包含算法名称版本、处理数据类型规模、核心逻辑摘要(需说明是否基于用户历史行为分配推荐权重、是否排除敏感数据等合规点)及风险评估报告的备案表；涉及高敏或极高敏数据的算法，还需经法学、数据安全与行业专家组成的评审组审核，通过后获取合规通知书，且每年度需提交迭代后的逻辑说明。

数据跨境传输可在“白名单 + 安全评估”基础上，参考《个人信息保护法》第 42 条细化规则。按保护水平将境外区域分类，等效保护区域可传输去标识化用户画像标签，基本等效区域需经第三方安全评估后传输脱敏核心数据，非等效区域仅允许传输完全匿名化统计数据，且需提交匿名化效果验证报告证明无法反向识别个人。

4.2. 企业合规体系的优化：从被动应对到主动防控

企业作为数据处理的主体，需构建全流程合规体系，将法律要求内化为经营逻辑。作者认为网络数

据库的营销信息系统需与企业管理架构深度融合，这一观点为企业合规体系提供框架思路。具体而言，企业应建立“数据治理–用户权利–技术保障”三位一体的机制：在数据治理层面，参考赵爱琴等在《论数据库营销》中提出的“数据更新与完善”原则，定期对营销数据库进行清洗，删除超出必要范围或过期的数据(如用户已注销账户的历史记录)，避免“数据囤积”风险；同时，明确数据处理的全流程责任人，从收集、存储到应用环节设置合规审核节点，例如在开展新的定向营销活动前，由专门团队评估其是否符合“最小必要”标准[6]。

在用户权利保障层面，需落实王菲倡导的“告知–选择”机制，通过简洁易懂的隐私政策(避免法律术语堆砌)向用户说明数据用途[9]，并提供可视化的权限设置界面——如王彤在其研究中提到的“一键关闭营销推送”功能，让用户能便捷撤回同意[5]。对于敏感数据的使用(如生物识别信息)，需单独弹窗提示并获得明确授权，而非默认捆绑在服务条款中。技术保障层面，应积极应用隐私计算技术，如通过联邦学习实现跨平台数据协同分析(各企业在本地保留原始数据，仅共享模型参数)，或采用差分隐私技术在用户数据中加入噪声，既不影响营销分析精度，又防止个体信息被识别。另外，数据挖掘伦理，也需融入技术设计中，例如算法模型应排除种族、宗教等敏感特征，避免歧视性营销。

4.3. 行业自律与社会监督的协同：从分散治理到多元共治

单一主体的合规能力有限，需依托行业组织与社会力量形成共治格局。行业协会应发挥积极职能，例如行业协会可制定统一的数据库营销标准，这一思路可进一步延伸为：由行业协会牵头制定《数据库营销隐私保护指南》，明确数据收集的红线(如禁止收集与服务无关的宗教信仰信息)、营销触达的频率限制(如同一用户每日接收广告不超过 3 条)，并建立违规企业黑名单制度，形成行业内的声誉约束。第三方监督机制的完善同样重要，参考美国的 Truste 认证模式，引入独立机构对企业合规情况进行审计，通过“隐私认证标志”向消费者传递信任信号——例如，通过认证的企业可在官网展示标识，未通过的则被公示，借助市场选择压力倒逼合规。用户是数据库营销中的对象，因此要尊重用户的权利，如开拓用户反馈渠道，也可纳入社会监督体系，建立跨平台的投诉处理机制，由行业协会汇总用户对营销骚扰、数据泄露的投诉，督促企业整改。此外，公众隐私教育不可或缺。大多数用户对数据价值的认知不足，这一问题可通过行业协会与媒体合作解决：制作通俗易懂的科普内容(如短视频讲解“Cookie 如何追踪行为”)，提升用户对隐私边界的判断能力；同时，推广“隐私–服务”价值交换的理性认知，让用户理解适度的数据共享可换来更优质的个性化服务(如精准推荐减少信息冗余)，从而在自愿基础上参与合规的数据库营销。

综上，数据库营销的合规路径需法律、企业、行业三方形成合力：法律提供刚性约束，企业构建内生合规能力，行业与社会补充监督短板，最终实现数据价值与隐私保护的共生共赢，这一目标的达成既需要借鉴国际经验，更需立足本土实践，在九份文献所揭示的技术逻辑、权利诉求与市场规律中寻找平衡点。

5. 结语

现有研究围绕数据隐私保护形成多维探索，但针对数据库营销场景的系统性分析存在明显缺口。有研究揭示“隐私终结论”的三重意涵，指出隐私保护是对技术社会的想象式抵抗，却未嵌入数据库营销的商业实践[10]；国内研究虽覆盖数据隐私保护的概念、技术、法律等维度，但整体处于起步阶段，缺乏对数据库营销全流程隐私风险的场景化拆解，合规路径实操性薄弱[11]。有研究区分隐私权与个人信息保护的法理差异，批判“知情同意”形式化困境，强调以权力制约平衡数据处理者与主体的不对等关系[12]，却未深入数据库营销“数据聚合–画像–推送”环节的权力失衡细节；蒋博涵提出的消费者数据治理“精

巧规制”模式，倡导多元主体协同与刚柔并济的治理手段[13]，却未针对数据库营销“数据共享链长、算法依赖度高”的特点设计差异化方案。另有研究指出算法信息茧房导致消费者控制权丧失，现有知情权、选择权难以应对治理需求，需强化结果控制与算法伦理，却未与隐私权边界界定形成联动[14]；从政策与法律治理二元框架出发，指出政策治理在创制权利、提供裁判依据上的局限，强调法律治理的可预期性与数据权利机制构建的重要性，却未具体到数据库营销场景下二者的衔接路径[15]。

本文立足上述研究基础，以数据库营销为具象场景，填补“泛化讨论多、场景细分少”“理论争议多、实操路径少”的空白，构建“隐私权边界界定–合规路径落地”的完整分析体系。理论层面，融合“隐私观念转型”与“隐私权–个人信息保护分立”逻辑，结合数据库营销中“主动收集与被动获取”的差异，将“传统隐私向信息隐私的跃迁”具象化为边界判定的场景变量，同时批判“一揽子同意”的形式化问题，通过“数据敏感度–处理目的–行业属性”的互动分析，将抽象权利区分转化为可操作的边界标准，既验证权利分立理论在商业场景的适用性，又弥补其缺乏场景化落地的不足。

实践层面，合规路径设计深度整合现有研究核心主张并实现突破：针对“精巧规制”的多元共治理念，细化为“法律场景化规则–企业‘数据治理–用户权利–技术保障’三位一体机制–行业自律指南”的分层方案，融入算法伦理要求，在企业技术保障环节增设“算法排除敏感特征”的审查节点，解决数据库营销中算法歧视与信息茧房的治理难题；针对“政策与法律衔接”命题，提出“政策引导行业标准制定、法律固化场景化规则”的协同机制，既强化法律治理的可预期性，又弥补合规对策实操性不足的问题。此外，通过解析数据库营销全流程的隐私风险，将“数据泄露的全生命周期风险”转化为针对性防控措施，推动数据隐私保护研究从“宏观框架”向“行业专项方案”迈进。

综上，本文在现有知识体系中的定位，是将分散的隐私观念理论、权利区分逻辑、治理模式构想整合并聚焦于数据库营销场景，形成“理论解构–场景分析–路径落地”的闭环；核心贡献在于，理论上为隐私观念转型、隐私权与个人信息保护分立等命题提供商业实践层面的验证，深化特定场景下的隐私边界理论；实践上构建的多维度合规路径，既吸收现有研究精髓，又针对数据库营销特殊性设计可落地规则，为企业合规与监管执法提供针对性指引，也为后续行业性数据隐私保护研究提供“场景化深耕”的方法论参考。

参考文献

[1] 王利明. 隐私权概念的再界定[J]. 法学家, 2012(1): 108-120, 178.

[2] 蔡奕端. 互联网精准营销中的个人信息保护研究[D]: [硕士学位论文]. 重庆: 西南政法大学, 2018.

[3] 胡云清, 曾菊兵, 刘生根. 世纪营销策略——互联网络数据库营销[J]. 北京工商大学学报(社会科学版), 2002, 17(2): 1-4

[4] 徐健. 浅析电子商务环境下的数据库营销[J]. 商, 2015(4): 94

[5] 王彤. 拥抱还是拒绝——大数据环境下精准营销的隐私问题探讨[J]. 视听, 2017(10): 104-105.

[6] 赵爱琴, 赵为, 衡凤玲. 论数据库营销[J]. 北京工业大学学报, 1998, 24(S1): 43-46

[7] 侯乐乐, 崔娜, 白向伟. 关于网络数据库营销若干问题的探讨[J]. 商场现代化, 2015(14): 58.

[8] 谢贵荣, 王晖. 浅论数据库营销[J]. 科学学与科学技术管理, 2003, 24(12): 38-40.

[9] 王菲. 互联网精准营销的隐私权保护: 法律、市场、技术[J]. 国际新闻界, 2011, 33(12): 90-95.

[10] 俞立根, 顾理平. “隐私已死”与技术社会的想象式抵抗[J]. 新闻记者, 2022(7): 58-70.

[11] 彭宁波. 国内数据隐私保护研究综述[J]. 图书馆, 2021(11): 69-75.

[12] 王苑. 数据权力视野下个人信息保护的趋向——以个人信息保护与隐私权的分立为中心[J]. 北京航空航天大学学报(社会科学版), 2022, 35(1): 45-57.

[13] 蒋博涵. 论我国消费者数据治理的精巧规制[J]. 财经理论与实践, 2025, 46(3): 148-154.

[14] 郭明瑞, 娄逸骅. 算法消费者信息茧房的治理困境与制度因应[J]. 深圳大学学报(人文社会科学版), 2025, 42(4): 86-95.

[15] 武西锋. 政策治理与法律治理——我国数据治理模式的反思与完善[J]. 北方法学, 2025, 19(4): 146-160.