E-Commerce Letters 电子商务评论, 2025, 14(12), 2208-2214
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124104

Hans汉斯

数据库营销中消费者敏感信息使用的合规问题研究

郁诗颖

贵州大学法学院，贵州 贵阳

收稿日期：2025年11月5日；录用日期：2025年11月20日；发布日期：2025年12月15日

摘 要

本文围绕数据库营销中消费者敏感信息使用的合规问题展开系统研究。在数字经济背景下，企业在利用敏感信息提升营销效率的同时，面临着日益严峻的合规挑战。文章基于《中华人民共和国个人信息保护法》等法律法规，从敏感信息的定义与特殊性出发，指出数据库营销中应遵循的合法必要、知情同意和安全保障三大原则。通过识别信息收集、存储分析和使用等环节中存在的过度收集、告知不清、同意瑕疵、安全措施不足及第三方共享风险等问题，结合典型案例进行深入剖析。研究进一步从法律监管、企业自律和消费者参与三个层面，提出构建多方协同的合规治理框架的具体路径，旨在平衡商业效率与个人信息保护，促进数字经济的健康可持续发展。

关键词

数据库营销，敏感信息，个人信息保护

Research on Compliance Issues in the Use of Consumers' Sensitive Information in Database Marketing

Shiying Yu

Law School, Guizhou University, Guiyang Guizhou

Received: November 5, 2025; accepted: November 20, 2025; published: December 15, 2025

Abstract

This paper undertakes a systematic exploration of the compliance issues associated with the utilization of consumers' sensitive information in database marketing. In the context of the digital

文章引用: 郁诗颖. 数据库营销中消费者敏感信息使用的合规问题研究[J]. 电子商务评论, 2025, 14(12): 2208-2214.
DOI: 10.12677/ecl.2025.14124104

economy, while enterprises are harnessing sensitive information to boost marketing efficiency, they are grappling with increasingly formidable compliance challenges. Grounding on laws and regulations, including the "Personal Information Protection Law", this paper commences from the definition and distinctiveness of sensitive information. It posits three fundamental principles that ought to be adhered to in database marketing: lawfulness and necessity, informed consent, and security safeguards. By pinpointing issues such as over-collection, ambiguous notification, consent irregularities, inadequate security provisions, and risks related to third-party sharing during the stages of information collection, storage, analysis, and application, this paper conducts an in-depth dissection in conjunction with typical cases. Furthermore, this research puts forward specific approaches for constructing a multi-stakeholder collaborative compliance governance framework from three dimensions: legal supervision, corporate self-regulation, and consumer engagement. The objective is to strike a balance between commercial efficiency and personal information protection, thereby facilitating the sound and sustainable development of the digital economy.

Keywords

Database Marketing, Sensitive Information, Personal Information Protection

1. 引言

在数字经济时代，数据已经成为重要的生产要素，在商业模式的创新与变革中发挥着重要作用。数据库营销作为企业精准化营销的重要手段，通过收集、存储和分析消费者数据，实现营销效益最大化。然而，这种营销方式高度依赖数据，需要对数据进行挖掘分析，尤其是在涉及消费者敏感信息时，不可避免地与敏感信息保护产生冲突。

近年来，个人敏感信息数据泄露事件频发，消费者对个人信息安全的担忧也日益加剧。在实践中许多企业在开展数据库营销活动时，未能充分尊重消费者的知情权与选择权，导致敏感信息滥用风险显著上升。这不仅损害了消费者的合法权益，也给企业自身带来声誉受损、法律诉讼及监管处罚等风险。国内学者对此类问题的研究主要可分为两种，一种如周雪峰、闫磊集中于对《中华人民共和国民法典》《中华人民共和国电子商务法》等法律的解读，分析法律条文对电商平台的合规要求[1] [2]。另一种如谢皓、张建文从营销角度，探讨精准营销、大数据“杀熟”等现象对消费者权益的侵害[3] [4]。

然而，现有研究多从宏观法律或抽象伦理切入，较少将法律要求、技术实现与电商具体营销场景相结合的系统性研究。本文研究将从这一视角切入，构建一个法律、技术、管理三位一体的分析框架。因此，本文在当前背景下研究数据库营销中消费者敏感信息使用的合规问题，具有独特的价值及意义。本文在现有研究基础上，对数据库营销的各个环节进行分析，说明合规风险，有利于促进数字经济的可持续发展。

2. 敏感信息合规使用的理论基础

2.1. 敏感信息的定义与特殊性

我国法律对敏感信息一词在法律上已经有官方定义，因此本文将基于法律定义展开讨论。根据《中华人民共和国个人信息保护法》(后称《个人信息保护法》)第二十八条规定，敏感信息是指一旦泄露或非

法使用，容易导致人格尊严受到侵害或人身、财产安全受到危害的个人信息。包括生物识别信息、宗教信仰、特定身份、医疗健康信息、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

当前个人信息权益已经超越简单的人格权益，成为可被利用的资源[5]。与一般个人信息相比，敏感信息具有其特殊性。敏感信息与信息主体的人格尊严、人身财产安全紧密相关，其泄露或滥用很可能造成歧视性待遇、诈骗勒索等情形，这些情形对消费者造成难以逆转的损害。而且敏感信息本身具有更高的隐私期待，所以应当基于此类信息更全面地保护。敏感信息处理活动也比一般信息处理风险更高，法律法规应当对其设定更严格的合规义务，在收集、存储、使用等各个环节采取更为审慎的保护措施。

2.2. 数据库营销中处理敏感信息的原则

数据库营销指企业搜集和积累大量的市场数据并对数据进行分析，以识别对某类营销活动或产品感兴趣的目标客户，再对目标客户进行关系维护与深度挖掘，并根据挖掘得到的信息制定和实施营销策略[6]。在数据库营销过程中处理消费者敏感信息，应当遵循合法必要、知情同意、安全保障的原则，这些原则是合规的基础。

合法必要原则是企业处理敏感信息的前提。该原则要求数据处理活动必须具有明确、合法的目的，且严格限于实现该目的所必需的最小范围。例如，健身类 APP 以提供个性化训练计划为由收集用户运动习惯数据可能具有必要性，但若进一步收集用户的政治观点或性取向等信息，则明显超出必要范畴。此外关于敏感个人信息合理使用规范基础的争议，即包含说与并列说之争议[7]。本文认为在合法合规使用敏感信息这一环节应当同时满足《个人信息保护法》第十三条的一般规则以及第二十九条的取得个人的单独同意条件。

知情同意原则，特别是单独同意规则，是敏感信息处理合规的重要环节。个人信息处理者在处理个人信息时，需遵循“知情同意”规则，即在收集、处理和利用个人信息前，必须向信息主体充分披露相关信息，并征得其明确同意[8]。与一般个人信息可能通过统一同意不同，法律要求处理敏感信息必须获得信息主体明确、自愿、充分的单独授权。企业不得采用默示同意、预勾选选项或捆绑授权等方式获取用户同意。授权告知应以清晰易懂的语言，明确说明处理敏感信息的目的、方式、种类及保存期限等，并尊重用户的自主选择权。减小部分应用在用户注册时因隐私政策授权过于冗长而一次性同意对所有信息的处理授权的可能性。然而，在一些特定情形下也存在例外，比如“汪某诉中国铁路成都局集团有限公司个人信息保护纠纷一案”[1]。法院认为，成都铁路局处理人脸信息符合《个人信息保护法》第十三条规定的不需要取得个人同意的例外情形，此时的人脸信息使用就不需要单独额外授权。

安全保障原则是指企业根据不同敏感信息的风险程度采取相应的技术和管理措施，确保敏感信息的保密性、完整性和可用性。其中既涉及数据加密、访问控制、匿名化处理等技术手段，也包括内部管理制度、操作规程和应急预案等管理措施。个人敏感信息的泄露可能导致消费者的基本权利受到负面影响，因此应当要求使用方在已经获得消费者授权同意的情况下进一步采取相应的技术手段以保障消费者的敏感信息不被泄露滥用[9]。

在数据库营销过程中处理消费者敏感信息，还应当遵循合法必要、知情同意、安全保障三大原则。这三大原则相互关联、相互支撑，构成一个有机整体，全方位多层次地保障消费者敏感信息。合法必要原则确立数据处理的边界和尺度，确保企业不会过度收集和使用敏感信息；知情同意原则允许消费者对自身信息进行支配，体现对个人意愿的尊重；安全保障原则为前两大原则的落实提供了技术和管理的支撑，确保敏感信息在整个使用过程中得到充分有效保护。

[1]参见央视网：全国首例！乘客起诉铁路部门刷脸进站侵权法院驳回，2021 年 1 月 7 日。

3. 数据库营销中各环节的合规风险识别

3.1. 信息收集环节

信息收集是数据库营销的起点，也是合规风险的高发区域。此环节风险主要表现为过度收集、告知不清和同意瑕疵。

过度收集指企业收集的敏感信息超出实现其声明营销目的所必需的范畴。部分企业出于数据囤积或发掘潜在商业价值的目的，广泛收集用户信息，忽视数据最小化原则。例如，许多 APP 均没有在没有逐项取得消费者单独同意的情况下，就进行敏感个人信息收集行为[2]。

告知不清则直接影响消费者的知情同意情况，许多企业的隐私政策采用冗长复杂、专业术语众多的法律语言，消费者难以真正理解其个人信息将如何被处理。尤其在涉及敏感信息时，若未以显著方式提示并说明处理规则及可能影响，告知的实质效果将大打折扣，进而影响消费者同意的有效性。在收集过程中，如果相关数据收集方式并不透明，消费者不知道自己的数据是如何被收集的，很难判断自己的数据安全是否受到保障[10]。因此，企业在收集消费者敏感信息时应当以普通大众能理解的语言，尽量简洁明了地说明信息收集范围、处理方式等关键信息，有助于消费者做出符合自己意愿的选择。

同意瑕疵是收集环节较为突出的合规风险。对于敏感信息，法律要求获取用户的单独同意。在单独授权中，被收集信息的主体可以单独就某项信息的处理要求信息处理人应当如实告知被处理信息的范围以及用途，确保被收集信息主体的知情同意[11]。然而实践中，部分企业仍通过一揽子授权将敏感信息与一般信息捆绑收集，或采用默认勾选等方式获取所谓用户同意。此种同意存在瑕疵，可能使后续处理行为失去合规基础。

3.2. 信息储存与分析环节

信息存储与分析环节的合规风险集中于安全措施不足、内部人风险两个方面。安全措施不足是导致数据泄露的原因之一。若企业未采取与敏感信息风险等级相匹配的安全防护措施，则极易成为网络攻击目标，引发大规模数据泄露。迪奥数据泄露事件中，企业未对收集的个人信息采取加密、去标识化等安全技术措施，正是安全措施不足的体现[3]。此外，平台信息也有被黑客恶意抓取的可能，从事网络黑灰产业务的魏某某，深知常规手段获取用户数据成本高、效率低，而开发“暴力获客”软件可低成本批量获取隐私数据。为了追求非法经济利益，2024 年年初，他向在网络上结识的擅长软件代码开发的谭某某提出定制软件要求，获得该软件之后，将之分级售卖给对用户个人信息有需求的电商从业者、小型直播团队，甚至于诈骗分子，在短短 5 个月时间，软件销量超过 1 万份。可以看出当前信息储存环节仍然存在较大信息泄露风险[12]。

内部人员带来的风险也不应该被忽视，企业员工，特别是拥有高数据访问权限者，可能因操作不当、意识薄弱或恶意行为导致敏感信息泄露。这些都是收集并使用消费者敏感信息的企业需要注意的问题。

3.3. 信息使用环节

信息使用环节是价值实现环节，也是滥用风险集中地，主要表现为超出授权范围使用、消费者权利保障不足及第三方共享风险三个方面。

超出授权范围使用是较为常见的违规行为。企业将基于特定目的收集的敏感信息用于未经用户授权的其他用途。在实践中，敏感个人信息处理不符合授权范围的表现多种多样。比如，对宗教信仰信息的

[2]参见南都个人信息保护课题组：《南都实测：多款 App 收集人脸等敏感信息未获单独同意》，《南方都市报》2021 年 4 月 30 日，第 6 版。
[3]参见央视网：法国品牌迪奥发生数据泄露事件，公安网安部门：予以行政处罚，2025 年 9 月 9 日。

采集，在绝大多数情形中均无收集以及使用的必要，只有宗教组织、政治组织才有必要处理此类敏感个人信息，然而相应数据仍然会被收集并使用[13]。

消费者权利保障不足会直接侵害消费者法定权利。《个人信息保护法》赋予个人知情、决定、查阅复制、更正补充、删除等方面的权益。但在实践中，企业可能未建立顺畅的权利响应机制。使用户难以查询企业存储了哪些自身敏感信息，并且在用户撤回同意后，企业是否及时停止使用并删除数据不得而知。在这些环节中消费者的敏感信息均泄露或被继续使用的风险。

第三方共享风险在商业合作情况下尤为明显。企业与合作伙伴共享数据时，若未签订严格数据保护协议、未对第三方能力进行尽职调查、或未向用户充分披露并获单独同意，一旦第三方发生数据泄露或滥用，原企业也可能承担连带责任。迪奥案例中“违规向法国迪奥总部传输用户个人信息”且“未取得用户‘单独同意’”，即暴露了跨境数据共享的风险。

4. 数据库营销中消费者敏感信息使用的合规路径构建

4.1. 法律与监管层面

首先，可以细化敏感信息处理规则标准。尽管《个人信息保护法》已经确立个人信息保护的基本框架，但相关配套规定和实施细则仍有待完善。各地政府可以针对当地特色、经济需要及企业特色对《个人信息保护法》设立相应的实施细则；监管机构可以针对不同行业特点，出台更具操作性的行业标准，通过进一步明确规定，对敏感信息处理的具体场景、合规要点和技术规范提出具体措施。如以“场景理论”为依托，进一步明确“单独同意”在不同交互场景下的具体实现方式，有效平衡信息主体与信息处理者之间的利益[14]。可以考虑将“单独同意”转化为动态、分层的同意管理，即针对不同的敏感信息使用场景，设计不同层级的同意选项，可以根据不同信息的使用场景，对其进行分层，并要求企业采取相应的保护措施。

其次，可以通过实施强化监管执法的精准度。相关机构应当对违法违规处理敏感信息的行为，特别是涉及面广、危害大的事件，依法采取严厉处罚。以实施促监管的同时，探索创新监管方式，鼓励合规创新。

最后，还可以推动隐私保护技术的研发应用。政府可通过政策引导鼓励差分隐私等前沿技术研究与应用，在保护原始数据不泄露前提下完成计算分析，为大数据营销与隐私保护共存提供可能，保护隐私的同时不放弃对经济发展的追求[15]。

4.2. 企业层面

企业作为处理消费者敏感信息的责任方，应当将合规要求贯穿于数据收集、使用和管理的每一个环节。在管理层面，企业应根据自身业务规模与面临的风险水平，制定切实可行的个人信息保护制度，明晰各部门职责，设立数据团队，将合规融入日常运营。可以将消费者个人信息进行分层，允许消费者自主选择信息公开程度。具体来说，可以将收货地址等信息归入基础功能层，授权使用该层信息可以使用软件内的购买物品功能。在体验增强层中采用单独弹窗询问是否获取与消费者个人相关的信息，如授权健康设备使用消费者个人身体数据用于个性化保健品推荐。最后在营销合作层面，再次单独弹窗询问是否同意将匿名的购物偏好与特定品牌商共享以获取专属优惠。并且配套设置动态同意与权限管理中心，在电商 APP 内设立一个常驻的、易于找到的“隐私偏好中心”，让用户可以随时、像管理手机 APP 权限一样，查看和调整对各类敏感信息处理的授权状态，并清晰看到不同选择对应的功能影响。

在技术层面，企业应在数据分类分级的基础上，对敏感信息采取加密、脱敏、访问控制等一系列强化安全措施，同时建立方便用户行使权利的相关辅助机制。在前端设计时使用图标化、可视化的语言解

释数据用途，避免长篇法律文本。采用明确的选择按钮，禁止预勾选。一旦用户撤回授权，企业应立即停止处理其敏感信息，同时通知相关第三方停止使用并删除数据。在数据分析阶段，优先使用差分隐私技术，在不直接接触原始敏感数据的前提下完成模型训练和用户画像。在与第三方合作层面，企业需要格外审慎，企业在共享敏感信息之前，应开展严格的调查，通过合同明确双方权责，并持续监督其数据保护情况，确保每一次数据共享都事先获得用户的单独同意和充分知情。此外，还应当定期开展数据保护影响评估，主动识别和防控数据处理活动中的风险，加强员工培训，提升全员的隐私保护意识与实操能力。

4.3. 消费者层面

消费者是自身信息权益的行使者，其自身维权意识提升和维权能力增强是倒逼企业推动敏感信息合规使用的重要力量。消费者应主动了解《个人信息保护法》等法律法规赋予的各项权利以及信息收集使用者应承担的义务。在日常生活中，谨慎处理个人敏感信息，认真阅读隐私政策，对非必要信息的授权索取保持警惕。积极行使法定权利，当发现个人信息权益受侵害时，消费者应勇于通过向网信等部门投诉举报、提起诉讼等合法途径维权。消费者的有效维权是对违法违规企业的警示，也是推动行业整体合规水平提升的社会监督力量。

5. 结论

本研究聚焦于数据库营销中消费者敏感信息使用的合规性问题，系统探讨数据库营销在数字经济背景下面临的现实挑战。研究发现，尽管数据库营销能显著提升商业效率，但在信息收集、存储、分析和使用的全流程中，仍普遍存在过度收集、安全措施不足、超范围使用以及用户权利保障不到位等合规风险。为实现商业效率与个人信息保护的平衡，本文提出应构建一个多层次协同治理体系，涵盖法律监管、企业自律与消费者参与三大维度。在法律层面，需进一步细化规则，引导企业合规应用技术。企业层面，应将隐私保护要求全面嵌入内部管理、技术实施与第三方合作流程。消费者层面，则应增强权利意识，积极行使自身信息权利。只有通过个人、企业与监管方的共同努力，才能构建起良性互动的合规生态，支撑数字经济的可持续发展。需要指出的是，本研究主要基于文献与法规分析，未来可进一步开展实证研究，并持续关注新兴技术对敏感信息保护带来的新挑战与应对路径。

参考文献

[1] 周学峰. 网络平台对用户生成数据的权益性质[J]. 北京航空航天大学学报(社会科学版), 2021, 34(4): 28-38.

[2] 闫磊. 大数据营销中的消费者隐私保护问题研究[J]. 市场瞭望, 2025(6): 1-3.

[3] 谢皓. 电商平台精准营销中个人信息侵权责任认定研究[D]: [硕士学位论文]. 青岛: 青岛科技大学, 2024.

[4] 张建文. 论自动化决策方式直接营销的个人信息法律基础[J]. 法律科学(西北政法大学学报), 2023, 41(6): 24-32.

[5] 王昱, 朱芝孺. 基于改进 K-近邻规则的数据库营销分析[J]. 统计与决策, 2018, 34(19): 175-178.

[6] 高富平. 个人信息保护: 从个人控制到社会控制[J]. 法学研究, 2018, 40(3): 84-101.

[7] 何红锋, 张宇轩. 敏感个人信息合理使用判定的法经济学分析——以个人健康信息为例证[J]. 安徽大学学报(哲社版), 2025, 49(6): 101-110.

[8] 闻志强, 施梦琪. 个人信息保护视角下知情同意原则的问题审视与完善路径[C]//上海市法学会.《法律研究》集刊: 智慧型开放的实现路径研究文集. 2024: 88-104.

[9] 刘畅. 我国敏感个人信息保护研究[D]: [硕士学位论文]. 济南: 山东政法学院, 2025.

[10] 徐翼. 生成式人工智能应用中个人数据安全风险及其法律规制路径[J]. 征信, 2025, 43(5): 9-16+28.

[11] 王利明. 敏感个人信息保护的基本问题——以《民法典》和《个人信息保护法》的解释为背景[J]. 当代法学, 2022,

36(1): 3-14.

[12] 卢晓琳, 顾敏. 个人信息被“开盒”用于营销[N]. 新华日报, 2025-10-20(004).

[13] 程啸. 个人信息保护法理解与适用[M]. 北京: 中国法制出版社, 2021: 267.

[14] 王鹏鹏. 论敏感个人信息的侵权保护[J]. 华中科技大学学报(社会科学版), 2023, 37(2): 41-51.

[15] 吕艳丽, 江伊雯, 冯函宇, 等. 基于差分低秩适配的大模型训练敏感信息保护方法研究[J/OL]. 计算机工程, 2025: 1-14. https://doi.org/10.19678/j.issn.1000-3428.00252845, 2025-11-02.