

电商平台“大数据杀熟”的法律问题研究

李明轩

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年10月15日; 录用日期: 2025年10月28日; 发布日期: 2025年11月26日

摘要

当今互联网技术发展迅猛, 电商平台依托大数据与算法技术, 实现了对消费者的精准画像与个性化服务推送, 极大地提升了用户体验与平台收益。然而, 部分商家滥用信息技术, 通过差异化的定价策略对用户进行价格歧视, 侵害了消费者合法权益的同时, 也扰乱了市场秩序。本文拟剖析“大数据杀熟”的基本内容, 阐明其具有技术依赖性、目标指向性及行为隐蔽性的特点, 进而从价格歧视说与算法歧视说两个维度探讨其法律属性。同时文章指出, “大数据杀熟”不仅违反了《消费者权益保护法》中关于消费者公平交易权的规定, 还侵犯了消费者的个人信息权益。文章通过对比分析欧盟与美国在“大数据杀熟”法律规制方面的实践经验, 提出了可能完善我国法律规制的路径, 包括修正知情同意原则、提供去标识化处理的技术保障、提升算法透明度以及设立专门的个人信息保护机构, 以期为保障消费者权益、规范电商平台经营行为提供支持。

关键词

电商平台, 大数据杀熟, 价格歧视, 法律规制, 消费者权益保护

Research on the Legal Issues of “Big Data Price Discrimination” on E-Commerce Platforms

Mingxuan Li

School of Law, Guizhou University, Guiyang Guizhou

Received: October 15, 2025; accepted: October 28, 2025; published: November 26, 2025

Abstract

With the rapid development of Internet technology, e-commerce platforms have leveraged big data and algorithm technologies to create precise consumer profiles and deliver personalized services, greatly enhancing user experience and platform revenue. However, some merchants abuse information

technology to implement differentiated pricing strategies, engaging in price discrimination against users, which infringes on consumers' legal rights and disrupts market order. This paper aims to analyze the basic content of "big data price discrimination," clarify its characteristics of technological dependence, targeted orientation, and behavioral concealment, and further explore its legal attributes from the perspectives of price discrimination and algorithmic discrimination. The paper also points out that "big data price discrimination" not only violates the provisions of the *Consumer Rights Protection Law* regarding consumers' right to fair transactions but also infringes on consumers' personal information rights. Through comparative analysis of the legal regulatory practices in the European Union and the United States regarding "big data price discrimination," the paper proposes potential paths to improve China's legal regulations, including revising the principle of informed consent, providing technical safeguards for de-identification, enhancing algorithm transparency, and establishing specialized personal information protection agencies, aiming to support the protection of consumer rights and regulate e-commerce platform operations.

Keywords

E-Commerce Platforms, Big Data Price Discrimination, Price Discrimination, Legal Regulation, Consumer Rights Protection

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

随着互联网的快速发展,人们日益频繁地借助各类网络应用程序,开展诸如购物、打车、订餐等多样化的日常活动。电商平台依托数据优势构建服务闭环,在提升用户体验的同时形成了稳定的盈利模式。但部分商家为追逐超额利润,将算法技术异化为价格操纵工具:通过非法抓取用户消费轨迹、构建动态定价模型,对忠实客户实施隐蔽的价格梯度调整,即行业所称的“大数据杀熟”[1]。从实际情况来看,该行为具有高度的隐蔽性,很难被消费者所知晓,且由于维权成本高昂,消费者在面对此类侵权行为时往往缺乏维权的积极性,这种消极态度在一定程度上又助长了该现象的泛滥,使其愈发猖獗,对市场秩序造成了极大的冲击。

2. 电商平台“大数据杀熟”的基本内容

大数据杀熟的主要表现形式为“针对不同用户设定差异价格”,也就是俗称的“一人一价”。例如,消费者通过同一电商平台订购一份曾经吃过的外卖,在菜品、预定时间等条件(未使用优惠券)均一致的前提下,价格却比首次购买的消费者要高;又如明明已经是某网店的VIP会员,结算价款时却显示比其他新用户价格还高等,这些案例无一不是“大数据杀熟”现象的典型写照。

2.1. 大数据杀熟的特点

1. 依赖性显著

大数据杀熟的本质是技术驱动的价格操纵。平台借助复杂的算法模型,对用户多维度数据进行深度解析,涵盖浏览轨迹、交易记录、搜索关键词等结构化与非结构化信息,并基于这些数据特征,为每位用户构建动态画像,据此实施分级定价策略。例如利用算法对用户的消费能力和价格敏感度进行预测,为价格敏感度低但消费能力强的用户设定较高价格。

2. 目标指向性明确

大数据杀熟具有极强的针对性，其核心目标群体为平台高黏性用户——包括长期活跃的老用户及品牌忠诚客户，这类用户因持续消费在平台积累了丰富的行为数据，为算法实施差异化定价提供了便利条件。相较于新用户或低频消费者，高黏性用户具有更强的平台依赖性与消费惯性，更换平台概率较小[2]。商家正是利用这一心理，通过大数据精准锁定此类群体，并针对其实施区别于普通用户的溢价策略。

3. 行为隐蔽性突出

大数据杀熟行为具有高度隐蔽性，其价格操纵机制往往难以被消费者察觉。一方面，价格差异通过算法隐式实施，平台既不会主动披露差异化定价策略，也不会建立用户间的价格比对机制，尤其在非标商品或服务场景中，消费者更缺乏横向价格参照体系。另一方面，平台利用复杂算法规则与动态定价模型，掩盖价格歧视的技术本质。例如，电商平台会以促销活动、库存变化、市场需求为由，对不同用户显示不同价格，将技术性价格操纵包装为市场波动现象，从而使消费者难以发现被“杀熟”。

2.2. 大数据杀熟的法律属性

1. 价格歧视说

价格歧视说，亦被称为差别定价说，在当下学界获得了多数研究者的支持与认同。持价格歧视说观点的学者认为，“大数据杀熟”并非随机定价行为，而是经营者借助先进的数据分析技术，深度剖析消费者多维信息，进而实施的高度差异化、精细化定价策略。从经济学理论来看，这种定价模式契合了“一级价格歧视”或“完全价格歧视”的特征。传统经济学中，一级价格歧视是一种理想状态[3]，即经营者能精准把握每个消费者的需求与支付意愿，为其设定独特价格，将消费者剩余完全转化为自身利润，实现收益最大化。“大数据杀熟”通过算法技术，使这种理论构想在数字市场中获得了部分映射。

2. 算法歧视说

从算法的视角剖析，部分学者主张将“大数据杀熟”这一经济现象在法律框架下界定为算法歧视的典型形态。在传统法律认知里，法律所明令禁止的歧视类型主要聚焦于性别、种族、宗教信仰等领域。然而，随着互联网技术的迅猛发展以及算法技术的不断精进，歧视的内涵与外延已不再局限于传统维度。算法凭借其“黑箱”特性，在消费者毫无察觉的情况下完成深度特征提取，构建详细的“数字画像”实施差别化定价[4]，这种基于算法技术的新型价格操纵行为，实质上构成了数字经济时代歧视的新形态。

3. 电商平台“大数据杀熟”的违法性分析

3.1. 侵害消费者的公平交易权

消费者享有公平交易权。我国《消费者权益保护法》第十条规定消费者享有公平交易的权利，即有权要求商品或服务价格合理透明无欺诈，且交易过程完全基于自愿。

然而当前盛行的“大数据杀熟”现象，实质上构成了对这两者的侵害。从交易条件的公平性维度分析，“大数据杀熟”是经营者通过动态定价模型收集用户数据，形成差异化价格矩阵，导致消费者在信息不对称状态下被迫接受的不合理定价，这种技术性价格歧视直接破坏了《消费者权益保护法》确立的公平交易准则；从拒绝强制交易的自主性来说，消费者因对定价算法机制不知情而与经营者达成交易，这种看似“自愿”的行为，实则因剥夺了消费者基于充分信息行使拒绝权的可能[5]，违反了《消费者权益保护法》中“交易自愿”的核心要求，构成对强制交易拒绝权的间接侵害。

3.2. 侵害消费者的个人信息权益

消费者依法享有个人信息权益，这在我国《个人信息保护法》中有明确规定。依据该要求，信息处

理行为需满足三项核心义务：其一，信息处理者负有全面告知义务，须以清晰、易懂的方式向信息主体披露信息处理目的、方式及范围，确保信息主体在充分知情的前提下自主作出同意表示，严禁任何形式的强制或误导性授权；其二，信息主体对个人信息处理享有双重决定权，既可限定处理的具体范围，也可指定处理的具体方式，信息处理者必须严格遵循信息主体设定的处理边界；其三，当信息处理目的、方式或范围发生法定变更时，信息处理者须重新履行告知义务并取得信息主体的明确同意，未经重新授权不得擅自扩大处理权限。

然而在当今的互联网时代，个人信息的收集与应用门槛大幅降低，实践中平台通过非法获取、格式条款强制利用及不合理使用个人信息，侵害消费者权益的情况屡见不鲜。典型表现为平台常以“一揽子授权”或默认勾选方式，突破“合法、正当、必要”原则，强制获取用户非必要信息，用户若拒绝则无法进一步使用；即使用户勾选了同意，经营者若对格式条款内容进行补充变更也不会重新征求其意见。更为严重的是，部分平台利用这些信息通过算法实施价格歧视，形成“数据非法获取－条款单方变更－算法定向杀熟”的完整侵权链条，既违反了个人信息处理的最小必要原则，也构成对个人信息权益的系统性侵害。

4. 域外电商平台“大数据杀熟”的法律规制分析及启示

4.1. 域外法律规制分析

1. 欧盟

欧盟针对“大数据杀熟”行为的法律规制，兼顾了促进市场竞争与遏制违法的双重目标。早期，欧盟依托竞争法与消费者权益保护法，禁止具有歧视性、掠夺性的滥用市场支配地位行为，例如《不公平商业行为指令》明确列举了三十余种被禁止的做法，聚焦打击利用价格误导消费者的现象。与此同时，欧盟构建起以数据保护为核心的法律体系。2016年出台的《通用数据保护条例》(以下简称 GDPR)将多种数据处理行为纳入监管范畴，使基于算法的“大数据杀熟”成为明确的规制对象。与我国在法律适用上面临的困境不同，欧盟采用概括性立法模式，依托专门法律规范对数据保护问题进行统一治理，形成了以数据权利保障为核心的规制框架。

GDPR 的规制路径主要围绕用户个人数据保护与算法解释权的设立：在用户数据权益保护层面，GDPR 第二章确立了目的限制原则、数据最小化原则等七项基本原则；要求数据处理主体需获得用户明确授权并限定处理范围；赋予用户知情权等多项具有对抗性的权利；网络服务提供者必须事先对平台自动记录用户搜索痕迹、购物记录等数据的行为进行说明，并征得用户的同意。此外，GDPR 第 35 条创设了数据保护影响评估制度，强制要求对高风险的数据处理行为进行事前评估，推动经营主体与用户共同防控风险。在算法治理方面，欧盟率先确立了算法解释权制度。《数据保护指令》第 12 条赋予了用户了解数据处理逻辑的权利，GDPR 在此基础上设立了算法解释权，进一步要求控制者对自动化决策进行限制，用户可以要求其说明机理。该制度有效约束了“大数据杀熟”中的差异化定价算法，从而保障了用户的知情权与自主选择权。

2. 美国

与欧盟相比，美国针对“大数据杀熟”现象构建了更具弹性的规制体系，其核心聚焦于消费者隐私保护与算法责任追究两大方面。

在消费者隐私保护层面，美国采用“行业自律协同立法”模式，以《消费者权利隐私法案》(以下简称 CPBR)和《加州消费者隐私权法案》(以下简称 CCPA)为主要依据。CPBR 以信息获取的知情同意为基础，强制要求经营者明确披露信息收集的类型与目的，并构建场景化风险管控框架，规定仅能在特定场景下合理收集与存储信息，若信息处理不当，经营者需开展风险评估并采取补救措施。此举以动态保护

机制突破了传统以消费者单方同意为主导的静态保护模式[6]。CCPA 借鉴欧盟 GDPR 立法理念，赋予消费者制约经营者优势地位的权利，禁止经营者因消费者行使权利而差别对待，同时拓宽诉讼主体范围，给予加州检察长提起民事诉讼的权力，有效减轻了消费者维权的负担。

在算法治理维度，美国采取“分散立法结合行业自律”策略。2019 年提出的《算法责任法案》要求运用算法的私营企业设立内部评估委员会，并定期披露评估报告，以预防算法滥用。《线上用户欺骗性体验减少法》则强制经营者设立独立审查机构，监督应用程序运行，并向用户及联邦贸易委员会提交监督报告。此外，美国计算机协会发布的《关于算法透明性与可责性的声明》，从提升算法透明度角度解决算法权力滥用问题。同时，脸书、微软等科技巨头通过设立首席隐私官，加强对算法应用的内部监管。

4.2. 域外法律规制启示

有效规制“大数据杀熟”现象，关键在于紧扣个人信息处理规范与算法治理机制。对比欧盟与美国的法律实践，二者虽都将个人信息权利保障、数据处理者义务设定、监管体系构建及救济渠道完善作为规制重点，但具体路径的差异十分显著。

欧盟以数据保护为根基构建规制体系，其代表性法律 GDPR 确立了数据主体的知情权、删除权等核心权利，并对数据处理者施加了全流程合规义务。这一模式虽能有效约束数据滥用，却存在过度聚焦个人数据保护、忽视算法治理规范的问题，且严苛的合规标准抬高了企业的运营成本，给中小企业带来较大压力。美国则选择了更具弹性的规制路径，以消费者权益保护与算法责任追究为双重核心。在消费者权益保障方面，通过 CPBR 与 CCPA 构建动态保护机制；在算法治理领域，采用“分散立法 + 行业自律”模式，如要求企业设立内部评估机制、建立独立审查制度。不过，分散式立法可能导致不同行业适用标准有别，影响法律实施的统一性。

基于域外经验，我国个人信息保护立法可获得如下启示：在保护原则上，可融合欧盟与美国模式，构建契合数字经济发展的框架；在权利义务配置上，完善数据处理者的义务；在算法治理领域，吸收欧盟算法解释权制度，确立算法知情权，要求企业建立保障机制；在监管体制上，设立专门的个人信息保护机构，提升监管的专业性与有效性。

5. 电商平台“大数据杀熟”法律规制的可能路径

5.1. 完善知情同意原则

如前文所述，在欧盟颁布的 GDPR 中，知情同意机制呈现出强控制特征。依据其第 7 条规定，数据控制者须以书面形式获取数据主体的同意，且同意请求的呈现方式应具备清晰性与显著性，同时要赋予数据主体随时撤回同意的权利。这种严格的知情同意原则尽管强化了对个人信息的控制，但若直接移植，可能会对数据的流通与利用产生抑制作用，进而降低数据的应用价值。

基于此，可引入“弱同意”模式，并结合场景导向的风险评估理论对现有机制进行优化。建议统合调整知情同意原则，借鉴美国 CPBR 中的场景分析理论，增强数据主体对个人信息的控制力，防止数据被过度处理。具体而言，在评估数据主体自由意志时，需重点考察其同意行为是否涉及对个人信息的非必要处理，除要求“单独同意”外，还应明确信息主体需通过“明示同意”的方式表达意愿。建议采用“列举+动态评估”的框架区分信息使用场景，根据不同场景及阶段的特点，灵活确定同意方式[7]。对于个人信息的二次处理，仍需重新获取信息主体的明确同意，不得仅凭隐私协议等文件直接处理数据。

5.2. 提供去标识化处理的技术保障

去标识化技术主要是指通过技术手段对个人信息中可能导致数据主体被直接或间接识别的信息进行

处理,以便在保护个人隐私的同时不损害信息的实际应用价值。这种平衡是非常微妙的:既要确保信息的匿名性,以阻断不必要的个人隐私,又要保留其足够的特征,以供后续的数据分析和决策支持使用。建议制定一套详尽且统一的个人信息脱敏标准来规范去标识化技术,涵盖从数据收集、存储、处理到传输各个环节,确保个人信息在处理周期内的安全性。当数据主体对个人信息处理表示反对或提出拒绝请求时,相关处理者应当立即暂停相关处理活动,并采取严格的去标识化措施,以充分尊重和保护个人隐私权。此外,还需要配合建立和完善数据安全网、数据流向追踪系统以及其他必要的安全措施,从而有效预防和减少个人信息被不当利用的风险。

5.3. 提升算法透明度

算法需具备“合理的透明程度”。《个人信息保护法》第七条、第二十四条通过透明原则与自动化决策透明度义务,为算法透明度奠定了法律基础。就此而言,有国外学者提出“鱼缸式透明”,也即完全披露计算机源代码。这种方式虽能遏制算法“黑箱”现象,却对经营者要求极为严苛,从而影响决策效率,且公众也难以精准理解披露内容,还可能泄露商业秘密、威胁公众隐私,并非合理之选。所以,算法应呈现“合理透明”,即公开算法决策逻辑与重要信息,而非将源代码完全公开[8]。

算法解释权的设立同样十分必要。这一权利由欧盟学者提出,旨在解释算法决策过程和结果,欧盟的《数据保护指令》和 GDPR 均对此作出了规定。GDPR 第十三条、十四条明确指出,数据主体有权获知自动化决策涉及的有意义信息及可能产生的结果,且在自动化决策产生显著经济或法律影响时,有权行使算法解释权并提出异议[9]。《个人信息保护法》第二十四条第三款也有类似规定,这表明算法解释权在我国法律中已初步显现。不过,GDPR 与《个人信息保护法》中关于算法解释权内容的表述较为模糊。欧盟规定解释权的主体为数据控制者,且不适用于公共领域。从效率上说,数据控制者作为解释主体确实最为合适,但同时数据控制者易作出有利自身的解释,因此不妨适当扩大解释主体的范围、强化监督力度。此外,GDPR 规定算法解释权主要应用于私人领域,而公共决策自动化影响公共利益,后果严重,所以算法解释权的应用领域也可进行拓展。《个人信息保护法》可从解释主体、领域等方面对算法解释权进行细化和完善,以解决算法透明度难题。

5.4. 设立个人信息保护机构

当今互联网交易呈现出跨地域、跨领域的显著特征,对于“大数据杀熟”的监管,在实践中涉及了多个不同的部门,这种复杂的监管格局使得执法工作面临效率低下的困境。为此,建立专门的大数据监管机构,对数据处理活动进行全面且有效的监督,是解决该问题的可行方案。

域外经验为此提供了宝贵的参考。欧盟 GDPR 法规要求成员国设立专门的数据保护机关,同时设立 EDPB(欧洲数据保护委员会)来监督成员国数据保护工作、协助制定适用指南。欧盟还借助个人信息保护官制度,严格监管数据活动,明确其防止数据泄露等职责;美国 CCPA 构建了完备的数据处理监督制度,赋予加州检察长对违法行为开展调查与诉讼的职能。由此可见,独立的数据监督管理机构在解决个人信息难题方面优势显著。因此我国可建立专门的个人信息保护机构,集备案、审查等功能于一体,监管“大数据杀熟”并赋予算法监管权。

在专门个人信息保护机构建设过程中,独立性是执法客观公正的前提,专业性是高质量高效执法的保障。目前《数据安全法》与《个人信息保护法》拟由国家网信部门统筹执法,但其在独立性方面存在局限。GDPR 第 52 条明确数据保护机构履职应保持独立,且机构成员必须具备个人信息保护方面的经验、知识与技巧。我国构建专门数据保护机构时应围绕这两点,充分考虑行政级别、专业人才等因素,以破解执法难题,保障个人信息安全。

6. 结语

互联网技术的持续迭代让经营者愈发意识到用户个人信息、算法技术等对于企业实现盈利以及提升市场竞争力具有不可估量的价值。“大数据杀熟”作为现代社会持续发展过程中衍生出的热点现象，已然在学界引发了激烈的讨论。这种借助先进的互联网技术过度榨取用户的剩余价值以谋取私利的行为，违背了商业伦理的基本准则，遭到了社会各界的强烈谴责。网络空间绝非法外之境，数字经济必须在合法合规的框架上稳健发展。鉴于此，深入厘清“大数据杀熟”的法律属性，全面剖析我国现行法律在规制“大数据杀熟”方面存在的不足，显得尤为必要且紧迫。我们应从多个维度着手，例如完善知情同意原则，为用户提供去标识化处理的技术保障，大力提升算法的透明度以及设立专门的个人信息保护机构，以此强化规制的力度，切实保障用户的合法权益。

参考文献

- [1] 孙宇. 算法个性化定价: 经济原理、实施风险与法律规制[J]. 南方金融, 2023(7): 56-68.
- [2] 陈君巧. 电商平台“大数据杀熟”与治理对策研究[J]. 中国商论, 2023(20): 39-41.
- [3] 许身健, 郜庆. 反垄断视阈下的算法价格歧视问题[J]. 中国法律评论, 2022(3): 105-116.
- [4] 李美娇. 电商平台大数据“杀熟”中消费者公平交易权保护研究[D]: [硕士学位论文]. 石家庄: 河北经贸大学, 2023.
- [5] 张冰冰. 电商平台“大数据杀熟”侵权责任研究[D]: [硕士学位论文]. 鞍山: 辽宁科技大学, 2024.
- [6] 莫殷. 电商平台经营者“大数据杀熟”法律规制研究[D]: [硕士学位论文]. 重庆: 重庆邮电大学, 2022.
- [7] 金幼芳, 王凯莉, 张汀菡. 《个人信息保护法》视角下“大数据杀熟”的法律规制[J]. 浙江理工大学学报(社会科学版), 2021, 46(6): 693-701.
- [8] 刘梦宇. 电商平台算法歧视侵权责任认定研究[D]: [硕士学位论文]. 武汉: 华中科技大学, 2024.
- [9] 贾章范. 论算法解释权不是一项法律权利——兼评《个人信息保护法(草案)》第二十五条[J]. 电子知识产权, 2020(12): 49-61.