

电子商务平台数据隐私保护问题研究

吴晓波

贵州大学法学院，贵州 贵阳

收稿日期：2025年3月11日；录用日期：2025年4月1日；发布日期：2025年5月8日

摘要

伴随着互联网经济的迅猛发展，电子商务平台数据隐私保护问题已引发了全社会的广泛关注与讨论。当前电商平台数据隐私保护困境源于法律体系碎片化、技术漏洞、监管执行力度不足及用户权益保障机制缺失等多重因素。针对上述难题，我们应在用户层面，简化协议文本，保障用户行使权益路径，鼓励公众参与监督；在技术层面，以科学技术为依托，构建动态隐私数据保护体系；在法律层面，应对现有法律进行整合，对电子商务平台收集、处理隐私数据的边界进行限定；在监管层面，建立跨部门数据隐私保护协同机制，强化监管效能。

关键词

电子商务平台，数据隐私，个人信息保护，数据安全

Research on Data Privacy Protection Issues of E-Commerce Platforms

Xiaobo Wu

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 11th, 2025; accepted: Apr. 1st, 2025; published: May 8th, 2025

Abstract

With the rapid development of the Internet economy, the issue of data privacy protection on e-commerce platforms has drawn widespread attention and discussion throughout society. The current predicament of data privacy protection on e-commerce platforms stems from multiple factors, including the fragmentation of the legal system, technical vulnerabilities, insufficient enforcement of regulations, and the absence of user rights protection mechanisms. To address these challenges, we should, at the user level, simplify agreement texts, ensure users' access to exercising their rights, and encourage public participation in supervision; at the technical level, rely on science and

technology to build a dynamic privacy data protection system; at the legal level, integrate existing laws and define the boundaries for e-commerce platforms in collecting and processing privacy data; and at the regulatory level, establish a cross-departmental data privacy protection coordination mechanism and enhance regulatory effectiveness.

Keywords

E-Commerce Platforms, Data Privacy, Personal Information Protection, Data Security

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. 研究背景

互联网经济自 20 世纪末以来不断蓬勃发展,个人电子产品数量不断增加,移动应用不断成熟,客观上为电子商务的稳定发展创造了良好的环境,中国电子商务随之快速发展并在全球处于领先地位,具有一定的优势。从电子商务平台易趣网自 1999 年诞生,到现在淘宝、京东、拼多多等一系列成熟的电商平台,电子商务平台的快速发展见证了中国经济的繁荣。2025 年 1 月 17 日,中国互联网络信息中心(CNNIC)发布第 55 次《中国互联网络发展状况统计报告》(以下称:《报告》)。《报告》显示,截至 2024 年 12 月,网络购物用户规模达 9.74 亿人,较 2023 年 12 月增长 5947 万人,占网民整体的 87.9% [1]。

随着大数据分析、人工智能等技术的深度应用,电子商务平台正通过用户行为追踪、交易记录分析等方式构建庞大的数据资产库。有关数据显示,电商平台处理数据量早已突破 ZB 级别(1 ZB = 1024⁴ GB),涵盖用户个人信息、消费偏好、消费历史甚至基于已有数据推出用户的社交关系图等高度敏感数据。这种数据规模的扩张虽为精准推销、动态定价等场景提供了支撑,却也导致数据隐私风险呈现几何级增长。例如,某知名跨境电商平台因算法漏洞导致数百万用户地址、支付信息等数据隐私信息遭到非法爬取,暴露出数据利用与安全保障的严重失衡[2]。

2. 核心概念界定

2.1. 电子商务

我国立法对于电子商务的界定是动态发展的,早期商务部《电子商务模式规范》¹《第三方电子商务交易平台服务规范(2016 修正)》²都对电子商务进行了定义,但是具体概念界定并不一致,同时法律效力位阶较低,均属于部门规范性文件,指导示范意义不强。直至 2018 年《电子商务法》的颁布,立法第一次从法律层面对电子商务的概念进行界定,《电子商务法》认为电子商务是指通过互联网等信息网络销售商品或者提供服务的经营活动³。本文以《电子商务法》中对于电子商务的定义开展论述。

2.2. 电子商务平台

互联网平台可以根据功能、竞争和开发程度、用户互动程度等进行分类。鉴于功能是平台比较直观

¹ 参见 2009 年商务部《电子商务模式规范》第 2.1 条:电子商务定义为:基于互联网技术和网络通信手段进行货物或服务交易,并提供相关服务的商业形态。

² 参见 2016 年商务部《第三方电子商务交易平台服务规范(2016 修正)》第 3.1 条:电子商务定义为:交易当事人或参与人利用现代信息技术和计算机网络(包括互联网、移动网络和其他信息网络)所进行的各类商业活动,包括货物交易、服务交易和知识产权交易。

³ 参见《电子商务法》第二条。

的特点且相对客观,因此根据功能可以将互联网平台分为交易型、社交型和内容型[3]。按照上述分类,电子商务平台则属于交易型平台。电子商务平台作为互联网时代的核心商业载体,通过移动端应用、网页及小程序等渠道重构传统交易模式,以 B2B、B2C、C2C 等多元模式(含在线交易、信息发布、商务咨询、物流服务四大功能)连接企业、消费者及政府。其优势在于突破时空的限制,提供便捷高效的交易环境,商家可精准展示商品、获取流量并提升销量,消费者享受透明比价、多样化选择和增值服务,同时平台通过数字化流程降低交易成本、缩短周期并构建信任机制。

2.3. 数据隐私

与隐私相关的数据大致可以分为两类,即个人信息和个人数据。个人信息是通过电子或其他方式记录下来的、与已识别或具备可识别性的自然人存在关联的各类信息;个人数据则是借助电子手段或其他方式对个人信息所进行的记录呈现[4]。而处于二者交叉领域的数据隐私是指个人或组织在数据处理过程中,对于某些不宜公开的信息所享有的保护权利。其涵盖的经济信息、社交媒体活动等内容[5],极有可能成为未来情感计算技术发展的数据基础,数据主题将面临个人隐私遭受侵犯、自由平等权利受限等更多维度问题[6]。

电子商务平台数据隐私是指在电子商务活动中,在个体不受到外界不当干预的前提下,他对于其个人信息自主管理的权利[7]。电子商务平台数据隐私具体包括以下内容:第一,用户的身份信息如姓名、家庭住址、身份证号码等数据,构成了最基础的隐私数据内容。第二,用户的购物历史、购物偏好、浏览数据和交易信息等行为数据,是电商平台实施精确营销的关键信息资源。第三,银行账户、信用卡卡号、支付密码等支付信息直接影响用户的财产安全。第四,用户所在的地理位置、IP 地址,持有设备的 ID。在移动电商领域,用户的位置、IP、ID 数据对于实施大数据杀熟非常关键[8]。

3. 电子商务平台数据隐私保护问题分析

3.1. 用户维权难问题

3.1.1. 过度收集用户信息

过度收集用户信息主要表现为:第一,权限泛化滥用。平台通过移动端应用强制获取与核心功能无关的权限(如读取通讯录、相册访问、持续定位等),例如某头部电商 APP 要求用户授权麦克风权限以支持“语音购物”功能,实则用于后台环境音采集分析消费场景[9];第二,数据采集冗余。利用 SDK 埋点技术超范围收集用户行为数据(如页面滑动轨迹、输入法习惯),甚至通过跨平台数据关联构建全方位的用户画像;第三,技术隐蔽性增强。采用设备指纹和面容识别替代传统 Cookie,通过硬件参数、网络特征等不可见标识实现跨应用追踪,某第三方检测报告指出大量电商 APP 存在静默采集 IMEI、MAC 地址等敏感信息的行为;第四,合规规避策略。利用“功能捆绑”设计迫使用户让渡数据权限(如将支付功能与地理位置授权强制关联),或通过模糊化隐私协议诱导用户“一揽子授权”。

3.1.2. 用户知情同意形式化

平台企业普遍采用数万字篇幅的服务协议和隐私政策,其中专业术语堆砌、条款嵌套复杂的文本特征,与普通用户的阅读理解能力形成显著断层。根据九派新闻的报道,主流软件的服务协议和隐私政策平均字数超过 2.6 万字,完整阅读需耗时 65 分钟以上,但实际仅有极少的用户会通读条款[10]。更值得关注的是,平台通过“默认勾选同意”“一键捆绑授权”等设计,将数据收集权限与基础服务功能强制绑定,用户在未充分知晓数据处理范围、共享对象及存储期限的情况下,被迫让渡个人信息控制权。这种伪同意机制实质上架空了《个人信息保护法》第 14 条规定的“充分知情、自愿明确”原则,使数据收集

的合法性基础沦为技术性合规的装饰。

3.1.3. 用户维权成本高、举证困难

用户维权需承担三重结构性障碍，其一，技术性举证壁垒导致权利主张虚置。数据收集、存储与流转的隐蔽性特征，使普通消费者难以获取平台违规操作的直接证据，尤其在算法歧视认定、数据共享链路追溯等专业领域，用户因技术资源与信息控制权的绝对劣势陷入举证不能的被动境地。其二，法律成本、时间成本与收益严重失衡。诉讼需支付的高昂律师费、鉴定费等费用，往往远超个体隐私侵权的实际损失，形成“维权投入与救济回报倒挂”的畸形结构，迫使多数受害者放弃法律追责。其三，法律要件证明标准与数据特性存在根本冲突。传统侵权责任框架下“过错-损害-因果关系”的证明逻辑，难以适配数据侵权的多主体参与、跨平台流转特征，用户既无法锁定具体侵权主体，亦难以证明信息泄露与损害后果的直接关联性。

3.2. 技术安全问题

3.2.1. 技术漏洞导致隐私数据泄露

电子商务平台系统架构的复杂性导致身份验证缺陷、接口权限失控等技术安全隐患长期存在，为外部黑客攻击提供可乘之机，攻击者利用漏洞渗透至核心数据库，窃取用户身份信息、支付凭证、生物特征等数据隐私信息。同时，内部权限管理体系的不完善使得开发、运维等环节存在过度数据访问权限，员工操作行为缺乏有效监控与审计，极易引发内部人员违规导出或贩卖用户隐私数据。此类技术漏洞不仅导致个人信息在存储、传输过程中暴露于风险敞口，更使得泄露数据通过暗网交易、黑灰产业链条形成二次扩散，衍生身份盗用、精准诈骗等社会危害。在全球电商领域数据泄露事件中，大部分源于内部技术权限管理失控或第三方接口漏洞。更严峻的是，部分平台通过“用户协议”模糊隐私数据使用边界，将个人隐私数据二次加工后用于征信评估、保险定价等衍生场景，形成数据越界开发的灰色地带。

3.2.2. 数据跨境传输中的监管空白

国际间数据主权主张的冲突与区域性数据流动规则的割裂，导致平台难以建立统一的合规框架。部分国家基于“数据本地化”要求限制数据出境，而另一些司法辖区则通过“充分性认定”机制设置高门槛，更严峻的是，数据出境后的动态流转路径缺乏有效追踪机制，当信息经第三方云服务商、分包处理商等中间环节多次转存后，原始数据控制方既无法约束下游的数据使用目的，也难以响应用户的知情权、删除权等法定诉求。

3.2.3. 算法歧视

人工智能系统在目标数据收集、选择性过滤和目的性分析的过程中往往会有意识或无意识地嵌入个人或群体的隐含价值，继而在模型构建中不断叠加这种不公平，形成有偏的输出，最终外化为针对某个人或某类社会群体的不公正决策或行为，这就产生了算法歧视问题^[11]。算法歧视是一种以算法为手段来实施的歧视行为，主要在大数据环境中，自动化决策系统基于机器计算对数据主体进行决策分析。然而，由于数据和算法可能缺乏中立性，或包含错误、受到人为操纵等因素的影响，这些系统可能对数据主体实施差别对待，导致歧视性的结果^[12]。根据成因的不同，可将算法歧视分为基于外部原因形成的算法歧视和基于内部原有形成的算法歧视；根据产生的阶段不同，可将算法歧视分为产生于设计端、产生于学习端和产生于应用端的算法歧视；根据设计者主观故意的不同，可以将算法歧视分为有意识的歧视和无意识的歧视^[13]。

电子商务领域中算法歧视是电商平台基于从用户处获取的隐私数据，通过算法自动决策对不同个体或群体进行不公正的差别对待，导致用户在商品推荐、价格设定、服务获取等方面受到不公平、不公正

待遇的现象。电商平台通过歧视性算法强化既有的算法偏见，不仅剥夺用户的平等交易机会，更以“技术中立”为幌子掩盖其不透明决策机制，这就会形成通常所说的算法黑箱，使算法不具有透明性，受害者陷入举证无门的困境。在电子商务领域，大数据杀熟也是典型的由外部因素导致的算法歧视现象，具体表现为算法设计者和电商平台为了利益最大化，在制定定价算法时，针对不同人群使用不同的价格机制，即对平台经常使用者比平台初次使用者推送的价格高，这也就是我们通常所说的杀熟现象[14]。在国内部分电商平台的“大数据杀熟”案例中，算法模型通过分析用户设备型号、消费频率等数百个特征维度，实现差异化定价，价格偏差率最高达 37%。更值得警惕的是，部分平台将用户行为数据与外部征信、医疗数据库交叉匹配，构建“隐形评分系统”，用于限制特定群体的金融服务可及性。

电商领域中的算法歧视具有侵害手段隐蔽性高、侵害法益广泛复杂等特点，它对消费者最主要最直接的危害主要体现在，第一，在数据收集阶段，电商领域的算法歧视侵害了消费者个人数据和隐私权，电商平台收集消费者信息的范围，除了收集经过消费者同意的信息外，还会收集相关的关联信息和其他未经消费者同意的信息。数据信息是互联网时代商业化竞争的最优质资源，因此电商平台对消费者隐私信息的过度收集，在一定程度上可能会促进电商平台的商业发展与竞争，但却是以侵害消费者法益为代价的；第二，在特定商品推送阶段，电商平台根据收集的消费者数据隐私，给消费者推送喜爱或容易被消费者接受的产品，使得消费者陷入信息茧房之中，从而侵犯消费者的选择权；另一方面，电商平台强行推送特定商品亦会侵犯消费者的知情权；第三，在商品定价阶段，电商领域的算法歧视会侵害消费者的公平交易权，电商平台和商家利用与消费者的信息差，不同的消费者在购买同一件商品时会支付不同的价钱，这会带来大数据杀熟等算法歧视现象[15]。

电子商务领域中算法歧视不仅会侵害消费者权益，还会侵害电子商务市场的交易秩序和竞争秩序。电商平台通过歧视性算法对消费者进行差异化定价、流量分配或搜索结果控制，使消费者面临大数据杀熟、差异化定价等问题，导致消费者对电商平台的信任度下降，破坏电子商务市场交易的公平性。同时，算法歧视通过电子商务平台给予的流量优势，打造所谓的“爆款商品”，欺骗消费者购买，这同时会导致电子商务领域中小商家的曝光机会和生存空间被削弱，形成“强者愈强、弱者愈弱”的恶性市场格局。

3.3. 法律与监管问题

3.3.1. 现有法律体系监管碎片化

多部法律规范间存在职能交叉重叠，执法尺度难以统一，既催生监管套利空间，又造成行政资源重复消耗浪费。首先，多部核心立法间存在规范交叉与逻辑断裂导致法律适用混乱。《个人信息保护法》《电子商务法》《数据安全法》等基础性法律虽各自确立数据处理的合法性边界，但缺乏对“数据本地化”“跨境传输”等关键场景的协同规制，形成竞合与监管盲区[16]。其次，国际数据流动规则与国内立法的衔接障碍放大了制度性矛盾。区域性数据主权主张的冲突使得平台难以构建统一的合规框架，既需满足“数据本地化”的强制性要求，又面临“充分性认定”机制的高门槛限制，这种制度张力迫使企业在数据自由流动与合规风险之间陷入两难困境。

3.3.2. 监管主体权责不清，执法力度不足

在多头监管的格局下，网信、工信、市场监管及公安等部门依据《个人信息保护法》《电子商务法》等不同法律行使职权，但权责边界模糊与协同机制缺失导致监管重叠与真空并存[17]。这种权责嵌套不仅造成行政资源的浪费，更使得数据收集、共享、跨境传输等环节的违法行为因“监管协调不足”而长期滞留于灰色地带。从执法效能维度看，行政处罚标准模糊与罚款额度偏低，难以形成有效威慑，部分平台将数据违规成本内化为“合规弹性空间”，形成“违法收益高于处罚风险”的异化激励体系。更深层的

危害在于，执法力度地域性差异与阶段性强化监管特征，削弱了法律实施的统一性与持续性。

4. 完善电子商务平台数据隐私保护的对策建议

4.1. 用户权益保障层面

首先，政府部门应当立法规范电子商务平台推出的服务协议和隐私政策等文本，用清晰易懂的语言和可视化的图表代替冗长难懂的文本，明确规定电商平台收集隐私数据的范围和用途，并在电商平台 APP 中设置“一键授权管理”功能，允许用户查看、撤回或调整电商平台已获取的数据权限。其次，针对用户维权困境，全国人大及其常委会应探索制定电子商务平台隐私数据侵权的举证责任倒置规则，要求电子商务平台承担举证责任，否则就承担不利后果，降低用户维权成本。同时还需要立法禁止电商平台过度收集用户信息和滥用软件权限。此外，政府部门和电商平台应当加强用户隐私数据保护宣传教育，通过短视频、保护手册与风险提示等手段，帮助电商平台用户认识隐私数据的重要性，并引导用户采取有效手段保护个人隐私数据安全。最后，政府应当设立独立的评估机构，定期对电子商务平台的数据隐私保护情况进行评估，形成评估报告并向社会公示，通过公开透明的监督机制推动企业保障用户权益。

4.2. 技术安全层面

在技术与管理层面，电子商务平台、政府和相关自治组织应构建覆盖数据收集、存储、使用、共享的全链条隐私数据保护体系。在技术上，需优先部署端到端加密技术，对用户身份信息、生物特征、交易记录等敏感信息进行实时脱敏处理，同时实行隐私数据调用审批登记制度；推广隐私计算框架，在保证数据可用性的前提下实现“数据可用不可见”。在安全管理方面，需完善数据隐私治理制度，明确最小化的数据收集原则和数据保留期限，设立专人负责数据安全审计，定期核查第三方服务商的数据合规能力。同时建立动态风险预警机制，利用 AI 模型监测异常数据访问行为，结合大数据技术固化操作日志以备追溯，确保隐私保护措施与业务发展同步适配。

同时，针对电子商务领域中算法歧视问题，首先，政府和电商平台应推动算法透明化，研发算法可解释性工具，避免算法黑箱。其次，应对算法进行安全评估与备案，设置内容管理追责制度，比如歧视性算法应用者责任、禁止歧视性内容输出、算法纠偏衣服。再次，设置算法歧视“提示性”技术，当电商平台输出算法歧视时，能够识别算法歧视并提醒电商平台纠偏，并自动发送处理算法歧视记录到政府相关监管部门，在处理记录达到一定数量时，政府监管部门便对电商平台进行处罚。最后，政府监管部门也可以主动使用 AI 工具来监测电商平台的算法歧视行为，节约人力成本和提高监测效率，及时发现并通知电商平台纠正算法歧视行为。

4.3. 法律与监管层面

在法律规制层面，政府、电子商务平台、行业协会需要构建多层次的协同治理法律体系，强化电商平台数据隐私保护。首先，政府有关部门应当会同人大及其常委会应当完善立法衔接机制，系统地梳理《个人信息保护法》《网络安全法》与《电子商务法》等法律的适用边界，修改重复、有争议或指向不明确的法律条文，还需要明确具体地规定数据收集的最小必要原则和目的限制原则。其次，政府要健全监管执法体系，建立跨部门联合执法机制，赋予监管部门对电子商务平台数据跨境流动的监控权与审查权，推行分级分类的监管制度并根据平台规模设定不同的合规政策。最后，政府和电子商务平台、行业协会应推动法律与技术协同演进，通过立法引导科学技术的应用与边界，将数据脱敏率、加密传输合格率等指标纳入电子商务平台合规评估报告，建立技术标准与法治要求的动态适配机制。

在监管层面，政府和电子商务平台应构建“全周期监管、协同化治理、技术化赋能”的监管体系。首

先,政府部门在原有监管组织架构的基础上,设立跨部门的数据治理委员会——由网信、市监局、执法单位等监督部门人员组成,联合监督与执法。同时还应整合网信、市监局等部门的职能,通过权责清单制度明确数据收集、存储、共享、跨境传输等环节的监管主体与执法边界。其次,建立由政府主导、电商平台参与的执法标准与动态评估机制,政府监管部门可依据平台规模、平台类别、数据类型、风险等级等条件对电商平台实施差异化监管,制定电子商务平台数据隐私保护监管政策。最后,政府可与电子商务平台共同构建数据隐私监测系统,通过沙盒试验区验证创新技术可行性,联合行业协会制定数据安全自律规范,同时由网信部门牵头协商制定跨境数据流动国际协作机制,并搭建量化评估框架,实现监管策略的动态调整。

5. 结语

综上所述,在互联网经济时代,法律体系碎片化、技术体系滞后、监管执行力度不足及用户权益保障机制缺位等多重因素导致电子商务平台数据隐私保护当下的困境。针对上述难题,我们应在用户层面,简化协议文本,保障用户行使权益路径,鼓励公众参与监督;在技术层面,以科学技术为依托,构建动态隐私数据保护体系;在法律层面,应对现有法律进行整合,对电子商务平台收集、处理隐私数据的边界进行限定;在监管层面,建立跨部门数据隐私保护协同机制,强化监管效能。

参考文献

- [1] 中宏网. 截至 2024 年 12 月,我国网络支付用户规模达 10.29 亿人[EB/OL]. 2025-02-19. <https://www.zhonghongwang.com/show-451-372456-1.html>, 2025-02-27.
- [2] 北京国旭网络科技有限公司. 中国跨境电商店铺数据库出现漏洞,数百万用户身份信息泄露[EB/OL]. 2023-11-17. <https://zhuanlan.zhihu.com/p/667422751>, 2025-02-27.
- [3] 周楠,许昕,蔡梦雨. 互联网平台企业的成长路径:分类与特点[J]. 中国科技论坛, 2023(12): 84-95.
- [4] 苗泽一. 数据交易市场构建背景下的个人信息保护研究[J]. 政法论坛, 2022, 40(6): 55-65.
- [5] 王禄生. 情感计算的应用困境及其法律规制[J]. 东方法学, 2021(4): 49-60.
- [6] 马长山. 智慧社会背景下的“第四代人权”及其保障[J]. 中国法学, 2019(5): 5-24.
- [7] 牛苗苗. 移动电商环境下用户隐私保护策略研究[J]. 商场现代化, 2025(4): 11-13.
- [8] 刘涛. AI 训练数据收集环节的包容审慎监管研究[J]. 秦智, 2025(2): 44-46.
- [9] 周振宇. 电子商务中消费者权益保护的问题研究[J]. 中国商论, 2023(4): 53-55.
- [10] 九派新闻. 聚焦 315 梳理 15 款顶流 APP 的用户协议,总字数超 40 万,10 万字在讲如何收集用户信息[EB/OL]. 2023-03-15. <https://baijiahao.baidu.com/s?id=1760389708552838953&wfr=spider&for=pc>, 2025-02-27.
- [11] 闫坤如. 人工智能的算法偏差及其规避[J]. 江海学刊, 2020(5): 141-146.
- [12] 裴嘉良,刘善仕,钟楚燕,等. AI 算法决策能提高员工的程序公平感知吗?[J]. 外国经济与管理, 2021, 43(11): 41-55.
- [13] 张禹. 大数据时代算法歧视法律规制研究[D]: [硕士学位论文]. 兰州: 兰州大学, 2023.
- [14] 卜素. 人工智能中的“算法歧视”问题及其审查标准[J]. 山西大学学报(哲学社会科学版), 2019, 42(4): 124-129.
- [15] 沈香珺. 电子商务领域中算法歧视的法律规制研究[D]: [硕士学位论文]. 青岛: 青岛科技大学, 2023.
- [16] 龙卫球. 《个人信息保护法》的基本法定位与保护功能——基于新法体系形成及其展开的分析[J]. 现代法学, 2021, 43(5): 84-104.
- [17] 康卫东. 审慎监管、功能监管与行为监管:我国金融科技监管的三维构建[J]. 海南金融, 2022(10): 33-44.