

# 电子商务消费者的个人信息保护问题浅析

姚 娣<sup>1</sup>, 丁 毅<sup>2,3</sup>

<sup>1</sup>扬州大学法学院, 江苏 扬州

<sup>2</sup>江苏理华律师事务所, 江苏 扬州

<sup>3</sup>扬州大学法治社会研究院, 江苏 扬州

收稿日期: 2025年8月8日; 录用日期: 2025年8月20日; 发布日期: 2025年9月4日

## 摘要

大数据时代, 互联网技术的飞速发展和在电子商务领域的广泛应用, 显著增强了电商平台对消费者个人信息的处理能力。但这同时也加剧了个人信息权益受侵害的风险, 如非授权收集、过度挖掘、泄露与滥用等。这一态势使得消费者难以有效控制其信息流向, 亦对个人信息保护制度提出了严峻挑战。本文从电子商务领域中消费者个人信息保护的现实困境着手, 探讨在现有行政法框架下强化保护的必要性。通过对平台的收集、处理程序、行政监管机制等关键风险点的行政规制困境进行分析, 旨在提出系统化改善策略, 包括优化知情同意机制、加强监管执法效能、完善行政救济制度等, 以期更有效地发挥行政法在个人信息安全方面的保障作用, 切实维护电子商务健康发展秩序。

## 关键词

电子商务, 消费者, 个人信息保护

# A Brief Analysis of the Protection of Personal Information of E-Commerce Consumers

Di Yao<sup>1</sup>, Yi Ding<sup>2,3</sup>

<sup>1</sup>Law School, Yangzhou University, Yangzhou Jiangsu

<sup>2</sup>LIHUA LAW OFFICE, Yangzhou Jiangsu

<sup>3</sup>Institute of Rule of Law Society, Yangzhou University, Yangzhou Jiangsu

Received: Aug. 8<sup>th</sup>, 2025; accepted: Aug. 20<sup>th</sup>, 2025; published: Sep. 4<sup>th</sup>, 2025

## Abstract

In the era of big data, the rapid development of Internet technology and its wide application in the

文章引用: 姚娣, 丁毅. 电子商务消费者的个人信息保护问题浅析[J]. 电子商务评论, 2025, 14(9): 586-590.

DOI: 10.12677/ecl.2025.1492951

e-commerce field have significantly enhanced the ability of e-commerce platforms to process consumers' personal information. However, this also intensifies the risk of personal information rights being infringed upon, such as unauthorized collection, excessive mining, leakage and abuse. This situation makes it difficult for consumers to effectively control the flow of their information and also poses a severe challenge to the personal information protection system. This article starts from the special demands and practical predicaments of consumer personal information protection in the field of e-commerce, and explores the necessity of strengthening protection within the existing administrative law framework. By analyzing the administrative regulatory predicaments of key risk points such as the collection, processing procedures, and administrative supervision mechanisms of the platform, the aim is to propose systematic improvement strategies, including optimizing the informed consent mechanism, enhancing the effectiveness of regulatory law enforcement, and improving the administrative relief system, with the expectation of more effectively leveraging the role of administrative law in safeguarding personal information security. We must effectively maintain the healthy development order of e-commerce.

## Keywords

E-Commerce, Consumer, Personal Information 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

个人信息是已识别或可识别自然人的各种信息, 个人信息的流动既涉及自然人的权利和自由, 又涉及公共利益的实现和维护[1]。《中华人民共和国个人信息保护法》的颁布, 为保障个人信息主体的人格尊严与数据安全权益构筑了法治框架, 显著提升了个人信息保护的法治化水平。然而, 在电子商务活动高度数字化、个人信息处理日益复杂化的现实背景下, 监管实践仍面临诸多挑战, 例如, 平台在告知同意规则的执行、数据共享边界的管控等方面均存在落实难点。因此, 实现对电商消费者个人信息的充分保障, 核心在于有效落实行政执法机关在个人信息处理活动中的法定监管职责, 特别是针对电商平台的特殊合规要求, 并持续推动相关行政监管制度的体系化健全与精细化完善, 以平衡电商生态的发展与消费者权益的保护。

## 2. 电商领域消费者个人信息行政规制的现实基础与必要性

在当今大数据时代, 社会的信息化程度越来越高, 极大地促进了信息的高效存储、共享与传播, 深刻变革了经济社会运行模式。在电子商务领域, 这一变革尤为明显: 消费者借助互联网就可以迅捷地获取商品与服务信息, 实现购物、订票、传输等, 享受前所未有的便捷性; 电子商务平台及经营者依托海量的消费者数据优化经营策略、驱动商业创新; 同时, 丰富的在线行为数据也为行政机关实施精准治理与优化公共服务提供了有力支撑。然而, 这在给人们带来便利的同时, 与个人相关的信息如家庭住址、电话号码、身份证号等亦是会被暴露在网络之中。信息技术、特别是大数据、人工智能在电商场景下的深度应用, 使得消费者个人信息被滥用、泄露等侵害风险显著加剧。消费者对其购物行为、支付信息、位置轨迹乃至个人偏好等数据往往缺乏有效的控制, 一旦被不法分子获取, 可能引发精准诈骗、价格歧视(如“大数据杀熟”)等连锁风险, 更是会增加用户被“人肉搜索”甚至遭受“网络暴力”的可能性。这在数字经济环境中强化对电商消费者个人信息的保护, 成为一个亟待解决的关键议题。一些电商平台

更是会将用户的个人信息当作一种资本进行转卖与交易以攫取非法利益, 这都严重侵害了公众的合法权益。在这种情况下, 若不由法律加以规制, 用户就会长期处于自己的信息是否已经被泄露的担忧之中。且随着公民权利意识的加强, 信息主体对于能够主动高效规制个人信息处理者的不法处理行为有着日益增加的现实需求。

强化行政规制是防范电商领域系统性公共安全风险的必然路径。电子商务场景中数据流通的多主体参与性显著放大了个人信息泄露的风险, 此类风险已逐渐超越个体权益侵害范畴, 演变为精准诈骗产业链与市场信用失范等系统性公共安全威胁。政府被赋予了对个人信息的监管职能, 是个人信息保护的重要主体。互联网技术的迭代推动政府构建全域性数据监管体系, 为提高公共安全治理水平, 政府必须充分有效地行使职权, 落实监管职责, 预防可能会发生的或者处理正在发生的对个人信息的侵害行为。

### 3. 电商消费者个人信息保护面临的行政监管困境

#### 3.1. 个人信息的收集、处理程序不当

在电子商务场景中, 移动应用程序在初始使用时要求用户授权个人信息访问权限已成为普遍实践。用户个人有权知晓电商平台收集个人信息的范围、目的、使用方式等, 并有权选择是否对个人信息进行授权访问。但在个人信息已经成为新的生产力要素的当下, 掌握更多的信息也就意味着有了更大的竞争优势, 电商平台倾向于通过复杂条款设计扩大数据收集范围以维持竞争优势。具体表现为: 隐私政策常以冗长文本与专业化术语呈现, 用户需多次界面跳转方可查阅, 且关键数据处理条款被模糊表述, 实质削弱了《电子商务法》第 17 条要求的知情权的实现。在用户的使用过程中, 平台还会默认用户同意收集其个人的网页浏览信息并用以分析用户的购物偏好、投放定向的视频与广告。在“个性化推荐”的背后往往没有合理的个人信息收集、处理程序, 没有充分履行事前的告知义务。

#### 3.2. 个人信息保护的行政监管机制薄弱

行政机关作为个人信息的监管者, 承担着平衡个人信息权益保障与公共数据利用价值的双重职责, 让公民的个人信息在法律的监管下得以充分利用。但现行架构难以适应电子商务领域的的数据治理需求: 一方面, 我国对个人信息进行监管的部门比较分散, 监管职责被分散到不同部门, 缺乏明确的划分和界定。责任主体缺位会导致一些领域无人监管或者发生多重监管的问题, 难以有效履行对个人信息的保护职责。另一方面, 行政机关内部收集、处理个人信息的工作人员也缺乏严格的管控, 信息收集行为缺乏克制, 其操作方式与使用的技术手段也可能并未经过严格的监督测评, 这些都可能会造成政府的不当处理行为。例如, 政府在政务网站进行信息公开时, 由于操作不当未将公民个人信息去标识化使公民个人隐私被公示, 虽然在被发现后及时撤稿, 但在一定程度上也造成了信息泄露的风险。

#### 3.3. 个人信息保护的行政救济制度不完善

个人信息存在着巨大的经济价值, 这就意味着个人信息容易遭到侵害, 而救济制度就是保障信息主体的权利得以实现的重要手段。法律规定信息主体可以向政府部门进行投诉和举报以维护自身的合法权益。但信息侵害行为的隐蔽性较强, 在网络所遗留的个人信息数据可能瞬间便会在未经信息主体同意情况下被储存到无数终端。又或者在和朋友交谈时提到的某件商品, 翻阅手机讯息时便能看到相关推送, 想要进行投诉和举报却很难找出侵犯个人信息的源头。

个人信息被侵害时也可以通过行政诉讼、行政复议等进行救济, 但这限于行政机关在进行信息公开时泄露个人信息的行为, 对于个人信息被其他社会公众侵害的情况无法充分发挥作用。除了在侵害结果发生后进行救济之外, 也可以进行事先的预防, 但我国现行法律法规对公民个人信息权益的保护多以事

后保护为主, 缺少事先预防的手段和措施。

## 4. 完善电商消费者个人信息行政保护机制的路径探析

### 4.1. 完善个人信息的收集、处理程序

只有通过正当的程序才能求得正当的实体结果, 行政机关在收集、处理公民个人信息的过程中应将程序正当原则贯彻在过程中的各个阶段。在个人信息收集前信息处理者应充分履行告知义务, 通过告知文件等形式告知信息主体, 保障公民的知情权与自决权。在行政过程中充分考虑信息主体的合理意见, 保障公众参与的机会。信息被收集、处理后能保证信息主体的权利可以得到充分的救济。

对于电商平台, 正如前文所说, 其提供的个人信息保护协议、隐私政策等条款冗长, 这显然没有做到《个人信息保护法》第 17 条提出的“显著、清晰”的要求。所以应对告知协议的篇幅做出一定限制, 使用尽量简短、精练的语言告知其信息处理行为, 并交由相关监管部门进行审查, 以保证该告知协议呈现在社会公众面前时是能为一般人所理解的。只有审查合格的平台才能正常上线运营; 审查不合格的, 监管部门应当勒令其进行修改, 再次审查合格后平台才可继续运营; 多次审查不合格的, 监管部门可采取罚款、通报等手段予以惩戒<sup>[2]</sup>。电商平台必须采取必要的措施保护用户个人信息的安全性和隐私性, 防止信息被泄露、非法获取与使用。如加强员工的培训和教育, 培养员工的法律意识和个人信息保护意识, 对能够访问和处理用户个人信息的人员进行限制; 定期进行信息的安全审查, 并建立风险评估和应急响应机制, 及时处理和回应个人信息安全事件; 不断升级数据加密技术与硬件设备, 以保证用户的个人信息在运输和储存过程中的安全。

### 4.2. 健全个人信息的行政法监管机制

从一般个人信息处理的实践来看, 信息安全的风险日益增大, 通过行政监管手段来规范个人信息的采集行为十分必要。但以往的监管措施已经无法满足现实的需求, 社会亟需通过新的手段加大对个人信息保护的行政监管力度。

#### 4.2.1. 设立专门的行政监管机构

为了保护个人信息权益, 规范个人信息处理活动, 促进个人信息合理利用, 应建立对重要个人信息处理者的特别监管<sup>[3]</sup>。例如, 可以设立独立于其他政府行政机关、能够独立行使权力和履行职责的监管机构, 对一些较大的电子商务平台进行监管, 明确其权利和义务, 强化和落实平台责任, 要求平台采取措施保护网络中的消费者个人信息, 增加平台运行的透明度。抑或是加强对行政机关内信息处理者的技术措施与技术手段的监督, 确保其能够安全地收集、储存及流转个人信息<sup>[4]</sup>。

#### 4.2.2. 健全对个人信息侵权行为的全流程监督

就目前来看, 《个人信息保护法》《网络安全法》《消费者权益保护法》《电子商务法》等法律规范中均明确规定了监管部门有权对存在非法个人信息处理行为的电商平台给予警告、罚款、责令改正、没收违法所得、责令暂停或者终止提供服务等违法处罚措施<sup>[2]</sup>, 政府的监管职责也在进一步地被优化和落实。但个人信息的保护不应过度依赖于事后处罚, 事前和事中亦要进行有效的监管, 尤其是在信息主体个人可能注意不到的领域, 预防并排除潜在的威胁因素。对于个人信息的收集处理过程中出现的泄露、非法利用等情况应当有针对性地采取措施, 健全对侵权行为的责任追究机制, 加大对涉案信息处理者的处罚力度。

#### 4.2.3. 鼓励社会公众广泛参与监督

政府应充分调动公众的积极性, 积极发挥电子商务消费者的监督作用, 抑或是鼓励社会公众对电商

平台隐私政策的制定和实施情况进行监督,使公众能广泛参与到对个人信息的保护中。这在增强社会公众对个人信息的保护意识的同时,社会公众监督个人信息采集行为、举报侵害个人信息权的行为可以使泄露个人信息的电商平台得到应有的惩罚,降低个人信息被侵害的风险,也有利于督促政府部门或者其他组织和个人能够按照法律规定进行信息的收集和处理。

### 4.3. 完善个人信息保护的行政救济制度

面对大数据时代的新形势,行政诉讼和行政复议可能无法充分发挥作用。为了更好地对信息主体的权益进行救济,我们可以进一步完善行政法的救济制度,拓宽事先预防的渠道,增加数据主体对个人信息进行自主决定的方法与途径,对于可能会受到侵犯的相关个人信息预先进行隐藏与删除。对此,可以考虑被遗忘权制度的构建。我国《个人信息保护法》中规定了个人信息删除权,其与被遗忘权较为类似,但从第47条规定来看,只有在符合法定情形时,信息处理者才需要主动删除,或者按照信息主体的要求进行删除[5]。且“用于社会服务而被收集的信息”本身就不在删除权的范围内,所以存在凡涉及公共利益的纠纷都可通过此条抗辩而使私权陷于不利处境[6]。相较而言,被遗忘权则是一种更为积极的事前的权利主张,数据主体可以在使用互联网的过程中通过行使被遗忘权、依靠技术手段实现相关信息在互联网上的彻底删除。这里的“彻底删除”是指数据控制者不仅要删除本电商平台上相关个人数据的全部链接,还要找到其他众多的数据控制者删除与信息相关的一切文件,这样才能预防因为相关个人敏感信息被泄露而导致的一些不可控的严重后果。

## 5. 结论与展望

在数字经济时代,电子商务消费者的个人信息保护已成为公共安全治理的关键议题。党的二十大将“加强个人信息保护”作为提高公共安全治理水平的重要内容[7],正是认识到信息数据作为新型生产要素与战略资源的双重价值,强化对电商消费者的个人信息保护已经成为迫切的时代需求。对于个人信息安全可能会面临的风险,要不断完善相关法律法规,进一步提升电商环境的法治水平。行政机关应担负起个人信息保护者的责任,加强监管和执法力度,拓宽行政救济途径,规范大数据应用,为用户提供更安全、透明和可靠的电子商务环境。

## 参考文献

- [1] 叶岚. 从控制到合作:个人信息保护策略优化[J]. 中共天津市委党校学报, 2023, 25(4): 64-75.
- [2] 梁栋. 电子商务消费者个人信息保护的规范路径——基于6类12家电商平台隐私政策的实证研究[J]. 大连理工大学学报(社会科学版), 2022, 43(3): 102-112.
- [3] 李爱君. 重要个人信息处理者的特别监管——兼论《中华人民共和国个人信息保护法》第58条[J]. 中国政法大学学报, 2023(4): 56-67.
- [4] 孙海涛, 王红利. 民法典时代个人信息保护的行政法回应[J]. 行政与法, 2021(12): 66-71.
- [5] 王利明. 论个人信息删除权[J]. 东方法学, 2022(1): 38-52.
- [6] 王春业, 曾幸婷. 从行政法视角看被遗忘权的确立[J]. 北华大学学报(社会科学版), 2023, 24(3): 73-84, 53.
- [7] 习近平. 高举中国特色社会主义伟大旗帜为全面建设社会主义现代化国家而团结奋斗 在中国共产党第二十次全国代表大会上的报告 2022年10月16日[M]. 北京: 人民出版社, 2022.