E-Commerce Letters 电子商务评论, 2025, 14(12), 4756-4763
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124427

Hans汉斯

电商平台个人信息收集的法律困境与规制路径

何　瑾

贵州大学法学院，贵州　贵阳

收稿日期：2025年11月13日；录用日期：2025年11月25日；发布日期：2025年12月25日

摘　要

随着电子商务的发展，电商平台在运营过程中收集了海量用户个人信息，其在带来商业效率的同时，也引发了过度收集、违规使用等个人信息安全风险。尽管我国已构建起以《个人信息保护法》为核心的个人信息保护法律体系，但该体系在应对电商平台复杂多变的实践时仍面临挑战。通过分析电商平台个人信息收集呈现出的范围广泛性、方式隐蔽性与行为持续性等实践样态，剖析当前法律规制面临的四大核心困境，“告知－同意”规则流于形式、“最小必要”原则适用模糊、平台“守门人”责任落实难以及用户救济途径不畅。针对这些困境，提出相应的系统性规制路径，以期为平衡数据利用与权益保护、促进数字经济健康发展提供理论参考与实践指引。

关键词

电商平台，个人信息收集，法律规制，告知同意规则

Legal Dilemmas and Regulatory Pathways for Personal Information Collection on E-Commerce Platforms

Jin He

Law School, Guizhou University, Guiyang Guizhou

Received: November 13, 2025; accepted: November 25, 2025; published: December 25, 2025

Abstract

With the development of e-commerce, e-commerce platforms have collected massive amounts of users' personal information during their operations. While this has enhanced business efficiency, it has also given rise to risks related to the excessive collection and improper use of personal information. Although China has established a legal framework for personal information protection cen-

文章引用: 何瑾. 电商平台个人信息收集的法律困境与规制路径[J]. 电子商务评论, 2025, 14(12): 4756-4763.
DOI: 10.12677/ecl.2025.14124427

tered on the Personal Information Protection Law, this system still faces challenges in addressing the complex and ever-changing practices of e-commerce platforms. By analyzing the practical patterns of personal information collection by e-commerce platforms—characterized by broad scope, covert methods, and continuous behavior—this study examines the four core dilemmas currently confronting legal regulation: the "informed-consent" rule becoming a mere formality, the vague application of the "minimum necessity" principle, difficulties in enforcing the platform's "gatekeeper" responsibilities, and inadequate user redress mechanisms. In response to these challenges, the study proposes a systematic regulatory approach aimed at balancing data utilization with the protection of individual rights and providing theoretical insights and practical guidance to foster the healthy development of the digital economy.

Keywords

E-Commerce Platforms, Personal Information Collection, Legal Regulation, Informed-Consent Rule

1. 引言

随着互联网、大数据、人工智能等技术的飞速发展，电子商务凭借其突破时空限制、降低交易成本、优化资源配置的巨大优势，已深度融入国民经济与日常生活。2025 年 1 月 17 日，中国互联网络信息中心(CNNIC)发布的第 55 次《中国互联网络发展状况统计报告》显示，截至 2024 年 12 月，中国网民规模达 11.08 亿人，网络购物用户规模达 9.74 亿人，占网民整体的 87.9%。[1]电子商务交易活动产生了前所未有的海量个人信息。这些信息不仅包括基本的身份信息与交易信息，更延伸至浏览记录、搜索偏好、地理位置乃至生物识别信息等深度数据，电商平台通过收集、分析和利用海量用户个人信息，构建用户画像，实现精准营销、个性化推荐和风险控制，从而创造巨大的商业价值。

然而，这一过程也伴随着个人信息安全风险，电商平台个人信息收集环节的不规范行为频发，电商平台在个人信息收集方面的违规案例更多地以行政执法案例(被监管部门通报和处罚)的形式出现。根据国家工信部发布的《关于侵害用户权益行为的 APP (SDK)通报》，截止 2025 年 10 月 28 日，共已发布 51 批 APP、SDK 违法违规收集使用个人信息通报，[2]此外，也有一些消费者提起诉讼的司法案例 [3]，暴露出电商平台对于个人信息非法收集、过度收集、擅自使用、数据泄露等问题日益突出，不仅侵犯了消费者的隐私权、人格尊严与财产安全，引发身份盗窃、网络诈骗等次生危害，还严重破坏了市场信任体系，制约了数字经济的健康发展。尽管我国已相继出台《网络安全法》《数据安全法》和《个人信息保护法》，构建了个人信息保护的基本法律框架，尽管如此，法律的原则性规定与复杂多变的商业实践之间仍存在巨大张力。电商领域因其场景复杂、主体多元、技术迭代快等特点，使得法律在具体适用过程中面临诸多困境。

因此，系统性地梳理电商平台个人信息收集的法律困境，并探寻行之有效的规制路径，不仅具有重

[1]中国互联网络信息中心。第 55 次中国互联网络发展现状统计报告[R/OL]。2025-01-17。https://www.cnnic.net.cn/n4/2025/0117/c88-11229.html，最后访问时间：2025 年 11 月 6 日。
[2]中华人民共和国工业和信息化部：《关于侵害用户权益行为的 APP (SDK)通报(2025 年第 6 批，总第 51 批)》，2025 年 10 月 28 日发布，https://www.miit.gov.cn/jgsj/xgj/fwjd/index.html，最后访问时间：2025 年 11 月 6 日。
[3](2025)沪 0115 民初 20298 号；(2022)粤 01 民终 3937 号；(2021)浙 06 民终 3129 号。

要的理论价值，对于保护消费者合法权益、规范平台经济发展、构建公平诚信的网络交易环境也具有紧迫的现实意义。本文将从实践样态出发，分析其困境及成因，提出相应的规制方案，以期为相关立法完善和司法实践提供参考。

2. 电商平台个人信息收集的实践样态与法律规制框架

2.1. 电商平台个人信息收集的实践样态

在数字经济时代，个人信息已成为驱动电商平台运营的核心要素。实践中，电商平台对个人信息的收集已远非局限于完成一笔简单交易所必需的基本信息，其收集行为在范围、方式与持续性方面均呈现出日益复杂和扩张的态势，具体样态如下。

1. 收集范围的广泛性。为实现基本的交易履约，平台需收集用户的核心身份信息与交易信息，例如姓名、身份证号、电话号码、收货地址及支付信息等，此部分信息具有必要性与合理性。然而，电商平台的收集范围已超出必要限度，呈现出全景式记录的特征。这主要包括：(1) 行为信息，即用户在平台内的动态足迹，如搜索关键词、浏览记录、页面停留时长、商品点击、收藏、加购行为、历史购买记录、评价内容以及售后服务记录等；(2) 设备与环境信息，包括用户终端的 IP 地址、设备型号、操作系统版本、唯一设备标识符(如 IMEI/IDFA)、浏览器类型与传感器数据等；(3) 衍生推断信息，即平台基于上述原始数据，通过算法模型进行分析加工后形成的用户画像，例如用户的兴趣偏好、消费能力等级、价格敏感度、甚至社交圈子特征等。这种广泛的收集行为旨在构建高度细分的用户标签体系，为精准营销、个性化推荐及商业决策提供数据支撑，但其广泛收集、深度挖掘的实践，模糊了必要信息与衍生信息、商业利用与人格权益之间的界限，对现有个人信息保护的法律框架构成了实质性挑战，体现出技术应用与法律规制之间的张力。

2. 收集方式的多样性与隐蔽性。除用户主动填写的注册与交易信息外，大量个人信息的收集过程依赖于技术手段，在用户无感知或难以充分知情的情况下完成。一方面，平台普遍采用 Cookies、Web Beacon (网络信标)及嵌入第三方 SDK (软件开发工具包)等跟踪技术，不仅用于追踪用户在本平台内的行为路径，更实现了跨网站、跨应用的行为数据采集，形成对用户数字足迹的持续性监控。另一方面，平台通过设计冗长复杂、专业性极强的隐私政策文本，在用户注册或首次使用时采用“一揽子”授权模式，即用户若不同意其全部条款(包括广泛的个人信息收集与使用规则)则无法使用核心服务功能。这种“全有或全无”的选择模式，实质上架空了用户的同意权，构成一种变相的“强制同意”，导致知情同意的原则在实践中被虚化。

3. 收集行为的持续性。电商平台的数据收集活动并非一次性的静态事件，而是贯穿于用户注册、浏览、搜索、交易、售后、社交分享等使用服务的全过程，大量涉及用户行为轨迹与设备信息的收集行为通过技术始终在后台持续运行，用户在此过程中往往缺乏明显的感知与有效的控制能力。这种贯穿始终、无感化的持续收集，使得电商平台能够积累形成关于用户的海量时序数据链，进一步加剧了个人信息被过度采集和潜在滥用的风险。

2.2. 现有法律规制框架

为应对日益严峻的个人信息保护问题，我国通过系统性立法构建了层级化的法律规制体系。当前，该体系以《中华人民共和国个人信息保护法》为核心，《网络安全法》《数据安全法》《电子商务法》《消费者权益保护法》等相关法律形成协同支撑，共同为电商平台个人信息收集行为设立了基本的法律遵循。

1. 核心立法

《中华人民共和国民法典》在人格权编中明确了自然人个人信息受法律保护的基本地位，为个人信

息权益提供了民事基本法层面的依据。《个人信息保护法》作为一部专门性、综合性的个人信息保护立法，其颁布实施标志着我国个人信息保护制度进入新阶段。该法系统性地确立了以“告知–同意”为核心逻辑的个人信息处理规则框架，详尽规定了处理者的义务与个人的权利，并设定了严厉的法律责任。

具体而言，《个人信息保护法》通过第五至第九条确立了五项核心原则，分别是合法、正当、必要和诚信原则，目的限定原则，公开透明原则，质量保证原则及安全保障原则。通过第十三条、第十四条设立“告知–同意”规则，“告知–同意”规则被视为处理个人信息的核心合法性基础，要求处理者在进行信息收集前，必须以显著方式、清晰易懂的语言向个人明示处理目的、方式、种类及期限，并取得个人的充分授权。同时，该法在第四章专章赋予个人一系列权利，涵盖知情、决定、查阅、复制、更正、补充、删除等诸多权能，为个人控制其信息提供了法律武器。此外，《个人信息保护法》还为个人信息处理者设定了全面的合规义务，包括制定内部管理制度、采取安全技术措施、进行个人信息保护影响评估等，并配以包括高额罚款、责令暂停相关业务等在内的严格法律责任，形成刚性约束力。

2. 多部法律协同规制

在《个人信息保护法》的核心框架外，多部法律从不同角度对电商平台的信息处理行为予以协同规制。《中华人民共和国电子商务法》第二十三条及第二十四条规定，电子商务经营者收集、使用用户个人信息应遵守相关法律法规，履行明示义务，并保障用户的查询、更正、删除等权利，体现了电子商务特定场景下的合规要求。《中华人民共和国消费者权益保护法》第二十九条则从消费者权益保护角度，再次强调了经营者处理消费者个人信息时应遵循合法、正当、必要原则，并履行告知义务且征得同意。而《中华人民共和国网络安全法》与《中华人民共和国数据安全法》则从宏观的网络空间治理与数据安全管控层面，为个人信息安全提供了底层制度支撑，如网络运营者的安全保护义务、数据分类分级管理以及重要数据出境安全评估等机制，共同构筑了个人信息安全的防护底线。

3. 部门规章与国家标准细化规则

在法律法规之下，部门规章与国家推荐性标准进一步细化了操作层面的规则。例如，国家市场监督管理总局与国家网信办联合发布的《网络交易监督管理办法》，针对网络交易环境中的个人信息处理活动提出了更为具体的要求。尤为重要的是，尽管《信息安全技术个人信息安全规范》(GB/T 35273)属于推荐性国家标准，不具备强制法律效力，但其内容详尽具体，为“最小必要原则”、“告知–同意”规则的具体实施提供了明确的技术指引，因此在司法审判和行政执法实践中，常被作为判断个人信息处理行为是否合规的重要参考依据，对电商平台的合规实践具有实质性的指导价值。

尽管上述法律框架已初步建成，为规制电商平台个人信息收集行为提供了基本的规范依据，但面对电商平台信息收集实践的复杂性、动态性与技术性，现有框架仍显不足。法律的原则性规定在具体适用时常面临解释与落地的挑战，原则的抽象性与实践的复杂性之间存在显著张力，导致规制效果未能完全达至立法预期。

3. 电商平台个人信息收集的法律困境

3.1. “告知–同意”规则形式化

“告知–同意”规则被视为个人信息自决权的核心体现，但在电商平台的海量、实时数据处理场景下，这一规则正遭遇挑战，呈现出严重的形式化倾向。首先，在“告知”层面，电商平台通常通过格式化的隐私政策履行告知义务，而平台的隐私政策通常篇幅冗长、用语晦涩、充满法律和技术术语，普通用户既无时间也无专业能力去仔细阅读和理解[1]。这种“通知”更像是一种法律风险规避手段，而非真正意义上的信息透明。用户往往在未充分理解其内容的情况下点击“同意”，导致“知情”的前提不复

存在。其次，在“同意”层面，平台往往利用其优势地位，通过“全有或全无”的捆绑式授权、默认勾选、以及不同意则无法使用核心服务的强制索权等方式，架空用户的真实意愿[2]。用户为了获取服务，不得不进行“一揽子授权”，其同意并非基于真实、自主的意志，而是迫于无奈的“被同意”或“裹挟同意”。此外，同意的一次性与处理的持续性之间存在矛盾。用户的一次点击，往往被平台解读为对未来不确定、持续变化的个人信息处理活动的无限授权，这严重背离了同意规则的初衷[3]。

3.2. “最小必要”原则适用模糊

《个人信息保护法》第六条规定，处理个人信息应当具有明确、合理的目的，且应当与处理目的直接相关，采取对个人权益影响最小的方式，收集范围应限于实现处理目的的最小范围。此即“最小必要原则”。“最小必要”原则是限制过度收集的关键，但在电商平台复杂的业务生态中，何为“必要”难以清晰界定。平台常以提升服务质量、优化用户体验为名，扩张个人信息收集范围，导致收集行为超越实现产品或服务核心功能的直接需求[4]。

首先，“最小必要”是一个情境化的概念，难以用统一、量化的标准进行界定。何为“直接相关”？何为“最小影响”？例如，平台以“提升服务质量和安全性”为由收集用户设备的精确地理位置，此目的是否合理？收集范围是否超出了风控所必需？由于缺乏权威、细化的指引，平台和监管机构可能对此产生不同理解。其次，在商业利益的驱动下，电商平台倾向于对“必要”进行宽泛解释。为了进行更精准的用户画像和广告投放，平台可能认为收集用户的社交关系、安装应用列表等信息是“必要”的。这种对商业目的的过度追逐，极易导致信息收集范围的无限扩张，背离最小必要原则的立法初衷。工信部历年发布的《关于侵害用户权益行为的 APP 通报》中[4]，多次出现 APP 因“违反必要原则，收集与其提供的服务无关的个人信息”而被要求整改，此类问题在电商类 APP 中尤为突出。由于缺乏清晰、可操作的判断标准，监管机构在执法时常面临认定困难，容易产生裁量空间过大或执法标准不一的问题。司法机关在审理相关案件时，也往往需要依赖个案具体情况和技术专家的辅助判断，增加了法律适用的不确定性。这使得“最小必要原则”在一定程度上成为“纸面上的原则”，威慑力与指引作用未能充分发挥。

3.3. 平台“守门人”责任落实难

《个人信息保护法》第五十八条赋予提供重要互联网平台服务的处理者以特殊的“守门人”义务，但在实践中，该条款的落实存在多重障碍。首先，其适用前提模糊，条文中“重要互联网平台服务”“用户数量巨大”“业务类型复杂”等关键概念缺乏明确的量化标准[5]。这导致哪些平台应适用该条款存在不确定性，既可能造成监管过度，也可能导致部分大型平台规避严厉义务。其次，现行法律对电商平台与平台内经营者的责任划分不够明确。平台作为“个人信息处理者”与“守门人”，其对平台内经营者信息收集行为的监督义务、审核义务的范围与标准缺乏具体规定，导致实践中平台与商家相互推诿责任。比如，商家为完成订单配送、提供售后服务，需要直接处理消费者的个人信息(如收货地址、电话号码)。在此过程中，若发生信息泄露或滥用，平台是否应承担责任？根据《电子商务法》，平台对平台内经营者负有一定的管理义务，但该义务是否延伸至对商家个人信息处理活动的日常监督？实践中，平台常以“商家独立运营”为由，试图规避责任，而消费者则倾向于向更具赔偿能力的平台追责，引发诸多纠纷。同时，对于平台未尽到安全保障义务导致信息泄露的赔偿责任，法律未明确归责原则与赔偿标准，使得受害者难以获得充分救济。此外，电商平台个人信息收集的监管涉及网信、市场监管、工信部等多个部门，各部门虽有大致的监管职责分工，但缺乏明确的权责边界与协同机制。实践中，对于跨领域、跨环

[4]中华人民共和国工业和信息化部：《关于侵害用户权益行为的 APP (SDK)通报(2025 年第 6 批，总第 51 批)》，2025 年 10 月 28 日发布，https://www.miit.gov.cn/jgsj/xgj/fwjd/index.html，最后访问时间：2025 年 11 月 6 日。

节的侵权行为，容易出现监管重叠或监管真空的现象。例如，市场监管部门负责查处不正当竞争相关的信息滥用行为，网信部门负责个人信息保护的综合监管，工信部负责网络安全监管，但对于平台过度收集信息的行为，可能因职责划分不明确导致监管滞后。

3.4. 用户救济途径不畅

首先，部分用户对个人信息的价值认识不足，缺乏个人信息保护意识，认为提供个人信息是获取电商服务的必要代价，对平台的过度收集行为习以为常。部分用户不了解自身享有的个人信息权益，也不清楚维权的途径与方法，在权益受到侵害时往往选择忍气吞声。其次，部分用户担心维权会影响自身使用平台服务，或害怕遭遇平台的报复性对待，如账号封禁、服务限制等，导致不敢维权。最后，在个人信息权益受到侵害时，尽管用户敢于维权，也面临举证难、维权成本高、救济效果差的困境。一方面，个人信息侵权行为具有隐蔽性，用户难以证明平台存在非法收集、滥用信息的行为，也难以证明自身损失与平台行为之间的因果关系；另一方面，个人信息侵权案件往往涉及众多受害者，单个用户的损失较小，维权成本远高于收益，导致用户缺乏维权动力。此外，现有救济途径包括协商、投诉、仲裁、诉讼等，但各途径之间缺乏有效的衔接机制，投诉处理效率低下，诉讼程序复杂漫长，难以实现对用户权益的及时救济。虽然引入了过错推定原则和公益诉讼，但惩罚性赔偿的适用尚存争议，对平台的威慑力不足[6]。

4. 电商平台个人信息收集的规制路径

4.1. 增强“告知－同意”规则的实质有效性

通过立法修订明确告知的具体内容与形式要求，规定平台应采用简洁明了的语言、可视化的方式展示关键信息，避免冗长复杂的法律术语。摒弃“一刀切”的同意模式，转向基于风险、场景和关系的差异化规制。

首先，引入动态场景化同意机制。借鉴动态场景化理论，根据个人信息处理的不同阶段(收集、利用、流转、删除)和具体场景，设计差异化的同意机制。在信息收集阶段，对于敏感个人信息和超出初始目的的处理，应坚持强化版的明示同意。在信息利用阶段，若处理目的、方式未变，可考虑适用默示同意，但必须为用户提供便捷的退出机制。在信息向第三方流转阶段，则应采取更为严格的“双重同意”或“三重同意”规则，即需同时获得信息主体和前手处理者的同意。

其次，实施信息分类分级与差异化告知。依据信息的敏感度(如一般信息、重要信息、敏感信息)和平台业务类型(如网络销售、生活服务)，制定差异化的收集范围和告知标准。对于敏感信息和高风险处理活动，要求平台进行增强式告知，如采用分层式隐私政策、图标化提示、短视频解说等用户友好方式，确保告知的有效性。将“知情同意”从“用户责任”转向“平台义务”，要求平台以清晰、易懂的语言履行告知责任。

最后，探索“选择退出”模式在特定互惠关系中的适用。在平台与老用户等已建立稳定、互惠关系的场景中，为降低交易成本、提升效率，可以谨慎探索以“选择退出”模式作为“告知同意”的例外[7]。例如，平台基于用户以往的购买记录推荐同类新品或提供专属优惠，可视为互惠行为，允许平台在明确告知且提供显著便捷拒绝方式的前提下进行，但必须严格限制其适用范围，并保障用户的退出权。

4.2. 推动“最小必要”原则的可实操性

当前困境的根源在于原则性规定缺乏具体指引。首要的规制路径是推动从“原则宣示”向“规则细化”的转变。立法机构与标准化组织应协同合作，针对电子商务的不同具体场景(如用户注册、商品浏览、在线交易、售后服务、精准营销等)，制定并动态更新更具操作性的判断指南。例如，可以借鉴“分层同

意”理念，在国家标准《信息安全技术个人信息安全规范》(GB/T 35273)的基础上，进一步出台《电商平台个人信息收集最小必要标准指引》。该指引应明确区分核心业务功能与扩展功能，并采用“正面清单”与“负面示例”相结合的方式，具体阐明各类功能所必需的最小信息范围。例如，明确“实现商品交易核心功能所必需的信息”包括收货地址、联系人电话，而“用于个性化推荐或营销的扩展功能”则不得强制要求收集用户的设备唯一标识符或社交关系链，必须获得用户的单独同意。这能为平台合规提供明确预期，也为监管执法提供统一、客观的尺规。

其次，深化隐私保护理念，从源头嵌入合规要求。事后监管成本高昂且效果有限，根本之道在于将合规要求内化于技术架构之中。应强制要求电商平台将“隐私保护设计”理念贯穿于产品设计、开发和运营的全生命周期。这意味着，数据最小化原则应成为技术实现的默认选项。平台应积极采纳差分隐私、联邦学习、数据匿名化等隐私增强技术，在实现用户画像、广告投放等商业目标时，尽可能使用去标识化、聚合化的数据，而非收集和集中处理原始个人信息。通过技术架构的革新，可以从源头上最大限度地减少过度收集的动机和可能性，使“最小必要”从一项外部合规要求，转变为平台内在的技术逻辑。

最后，除了外部强制，还需激发平台的内生动力，形成多元共治格局。一方面，可探索建立合规激励制度，将平台遵守“最小必要原则”的情况纳入企业信用评价体系，与享受政策优惠、政府采购等挂钩，形成正向引导。另一方面，应充分发挥行业自律与公众监督的作用。鼓励行业协会制定严于国家标准的团体标准，并建立行业内的合规认证与监督机制。同时，畅通用户投诉举报渠道，定期向社会公布电商平台个人信息保护的合规“红黑榜”，将企业的合规表现与其市场声誉直接关联，利用市场力量形成强有力的外部约束。

4.3. 完善平台“守门人”责任的落实机制

首先，明确“守门人”的认定标准与具体义务。应通过配套法规或国家标准，对“用户数量巨大”“业务类型复杂”等概念进行量化界定，如参考欧盟《数字市场法案》，以月活跃用户数量等作为门槛。同时，细化四大义务的操作指南，如明确独立监督机构的内外部人员比例、议事规则、监督权限；规定平台规则中必须包含的商家个人信息处理规范；明确“严重违法”需停止服务的具体情形和程序等。

其次，构建平台与平台内经营者分级责任体系。针对平台与平台内经营者责任划分不清的问题，应依据风险控制原则，构建分级、分类的责任分配机制。在立法或司法解释中明确，电商平台作为“守门人”，其对平台内经营者个人信息处理活动的监督义务，应至少包括：(1) 制定统一的平台规则，明确要求平台内经营者遵守个人信息保护法规；(2) 建立准入审核与定期巡查机制，对经营者的隐私政策、信息处理能力进行基本审查；(3) 设立便捷的投诉举报渠道，并对查实违规的经营者采取限制流量、暂停服务直至清退等处置措施。

最后，应对多头监管困境，需建立高效的部门协同执法框架。建议确立网信部门作为个人信息保护领域的牵头主管机关，负责统筹协调对大型平台的日常监管与专项检查。同时，建立常态化的信息共享、线索移交与联合执法机制。例如，市场监管部门在查处“大数据杀熟”等不正当竞争行为时，若发现平台存在过度收集信息问题，应及时将线索移交网信部门；工信部门在 App 合规检测中发现的问题，也应与网信部门共享。通过建立统一的监管信息平台，明确各部门在个人信息保护全链条中的主责与辅责，形成监管合力，彻底消除监管重叠与真空。

4.4. 构建便捷有效的权利救济体系

当前用户在面对电商平台个人信息侵害时呈现出的“不愿维权、不敢维权、不能维权”之困境，暴露出权利救济机制在实效性上的严重不足。为扭转用户个体的弱势地位，确保《个人信息保护法》赋予

的权利不止于文本，须构建一个低成本、高效率、强支撑的多元救济体系。

首先，破解“不愿维权”困局，需从源头提升用户的权利认知与自我保护能力。监管机构、消费者协会及平台应承担起普法宣传责任，通过发布通俗易懂的指南、典型案例和警示视频，向公众清晰阐释个人信息权益的内涵、平台合规义务的边界以及维权的具体流程。此外，应鼓励和推广技术赋能工具的开发与应用，例如浏览器插件或手机应用，帮助用户一键检测、管理乃至记录平台的个人信息收集行为，将复杂的侵权判断转化为可视化的风险提示，为用户行使“知情权”和“同意权”提供技术辅助，变被动忍受为主动管理。

其次，消除用户“不敢维权”的恐惧，关键在于斩断平台可能的报复链条。监管部门应出台明确规定，将无正当理由对维权用户进行差别对待(如限流、封号、提价)等行为界定为新型的、恶劣的违法情形，并设定严厉的行政处罚。同时，应建立匿名或集体投诉渠道，允许用户在不暴露个人身份的情况下举报平台违规行为。此外，可探索设立维权者保障基金，为因维权而遭受实质性损失的用户提供临时性救济，并通过权威渠道公开曝光打击报复的典型案例，形成强大威慑，为用户营造一个安全、无后顾之忧的维权环境。

最后，针对“不能维权”中的核心障碍，需对诉讼制度进行针对性改良。一是全面强化举证责任倒置规则的适用。在司法实践中，应严格落实《个人信息保护法》的过错推定原则，一旦用户提出初步证据，即由平台承担其信息处理行为合法合规的举证责任，彻底将用户从难以完成的举证负担中解放出来。二是积极探索和创新集体诉讼模式。应简化集体诉讼的启动条件，鼓励消费者协会、检察机关乃至符合条件的律师团队提起个人信息保护公益诉讼，将分散的、微量的个体损害汇聚成有影响力的集体诉求，实现“小额多数”侵权行为的规模化救济，大幅提升维权效益。三是细化惩罚性赔偿与法定赔偿规则。在难以证明实际损失时，应推广适用法定赔偿，并明确将平台的过错程度、获利情况作为计算赔偿额的考量因素，显著提高侵权成本，使维权行为具有经济上的可持续性。

5. 结语

电商平台个人信息收集的规范治理，是数字时代背景下平衡技术创新与权益保障、激发市场活力与维护公平诚信的关键课题。通过研究表明，我国个人信息保护的法律框架虽已确立，但其原则性规定在应对电商平台的具体实践时，在规则落地、责任划分与权利救济等方面均存在显著的张力与滞后性。破解“告知–同意”形式化、“最小必要”模糊化、“守门人”责任虚化及用户救济弱化等困境，无法依靠单一的法律条文修订，而需采取一种多维度、系统性的治理思路。未来的规制路径应致力于实现从静态立法向动态治理的转变，将法律标准的细化、技术手段的赋能、监管模式的创新以及多元共治机制的构建有机结合。唯有如此，才能将纸面上的权利切实转化为守护用户个人信息安全的坚实屏障，最终推动平台经济在合规、健康的轨道上行稳致远。

参考文献

[1] 袁莹莹. 网络平台个人信息“告知同意”规则的困境与出路[J]. 网络安全与数据治理, 2024, 43(10): 83-90.

[2] 徐伟, 李文敏. 数智时代 App 收集个人信息的安全风险与法律应对[J]. 山东行政学院学报, 2025(1): 113-121.

[3] 夏庆锋, 戴媛媛. 个人信息处理同意规则的动态场景化完善[J]. 安徽大学学报(哲社版), 2025, 49(5): 113-122.

[4] 徐伟, 李文敏. APP 个人信息收集风险治理: 欧盟经验及启示[J]. 南京邮电大学学报(社会科学版), 2025, 27(3): 21-30.

[5] 杨赵颖. 平台个人信息保护义务的困境与纾解[J]. 河北法律职业教育, 2025, 3(6): 89-94.

[6] 卜玲玉. 个人信息过度收集行为的相关问题及法律规制[J]. 法制博览, 2025(21): 118-120.

[7] 孙鸿亮. 基于自动化决策的商业广告的法律规制[J]. 中国法律评论, 2025(4): 196-210.