E-Commerce Letters 电子商务评论, 2025, 14(11), 2634-2639
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113729

Hans汉斯

电子商务中消费者个人信息保护的现实困境与完善路径

薛双怡

贵州大学法学院，贵州 贵阳

收稿日期：2025年10月14日；录用日期：2025年10月29日；发布日期：2025年11月27日

摘 要

互联网技术的迭代与数字经济的崛起，推动我国电子商务领域进入高速发展阶段。在电商生态中，消费者个人信息是商家优化服务、实现精准营销的核心资源——从注册账号时的基本信息，到交易过程中的消费记录，再到浏览行为产生的偏好数据，这些信息共同构成了电商运营的“数据基石”。然而，随着个人信息价值的日益凸显，个人信息保护的问题也逐渐暴露出来。尽管2021年施行的《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)与2019年实施的《中华人民共和国电子商务法》(以下简称《电子商务法》)构建了个人信息保护的基础法律框架，但实践中仍存在法律细则缺位、行业自律薄弱、消费者维权困难等问题。本文结合现有研究与立法实践，系统梳理电子商务中个人信息的特征与受侵害形态，剖析保护困境，并提出多维度完善对策，以期为电商领域个人信息保护体系的优化提供参考。

关键词

电子商务，个人信息保护，完善制度

The Practical Dilemmas and Improvement Approaches in Protecting Consumers’ Personal Information in E-Commerce

Shuangyi Xue

School of Law, Guizhou University, Guiyang Guizhou

Received: October 14, 2025; accepted: October 29, 2025; published: November 27, 2025

Abstract

The iterative development of Internet technology and the rise of the digital economy have propelled

文章引用: 薛双怡. 电子商务中消费者个人信息保护的现实困境与完善路径[J]. 电子商务评论, 2025, 14(11): 2634-2639. DOI: 10.12677/ecl.2025.14113729

China's e-commerce sector into a stage of rapid growth. Within the e-commerce ecosystem, consumers' personal information serves as a core resource for merchants to optimize services and achieve precise marketing—from basic information provided when registering an account, to consumption records during transactions, to preference data generated through browsing behavior, all of which collectively form the "data cornerstone" of e-commerce operations. However, as the value of personal information becomes increasingly evident, issues surrounding personal information protection have gradually emerged. Although the *Personal Information Protection Law of the People's Republic of China* (hereinafter referred to as the "*PIPL*"), implemented in 2021, and the *E-Commerce Law of the People's Republic of China* (hereinafter referred to as the "*E-Commerce Law*"), implemented in 2019, have established a basic legal framework for personal information protection, practical problems remain, including gaps in legal details, weak industry self-regulation, and difficulties for consumers in safeguarding their rights. This paper, combining existing research and legislative practice, systematically summarizes the characteristics and forms of infringement of personal information in e-commerce, analyzes the protection dilemmas, and proposes multidimensional measures for improvement, aiming to provide reference for optimizing the personal information protection system in the e-commerce sector.

Keywords

E-Commerce, Personal Information Protection, Improvement System

1. 引言

互联网技术迭代与数字经济崛起推动我国电商高速发展，据商务部《中国电子商务报告 2020》，2020 年全国电商交易额达 37.21 万亿元，网上零售额超 11.76 万亿元，电商已成国民经济重要增长极。在电商生态中，消费者注册信息、消费记录、浏览偏好等个人信息是商家优化服务、精准营销的核心资源，但信息价值凸显的同时，保护危机加剧：中国互联网络信息中心(CNNIC)第 49 次报告显示，截至 2021 年底，我国 10.32 亿网民中 22.1%遭遇个人信息泄露。

尽管 2021 年《个人信息保护法》与 2019 年《电子商务法》构建了基础法律框架，但实践中仍存在法律细则缺位、行业自律薄弱、消费者维权困难等问题，且跨境电商、大数据共享场景下，个人信息跨境流动法律冲突、"同意疲劳"致权利架空等新挑战涌现。基于此，本文结合研究与立法实践，梳理电商个人信息特征及受侵害形态，剖析保护困境并提出多维度对策，为电商个人信息保护体系优化提供参考。

2. 电子商务中个人信息的界定与核心特征

2.1. 个人信息的法律界定

根据《个人信息保护法》第 2 条，个人信息是指"以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息"。在电子商务场景中，这一界定需结合交易全流程理解：既包括直接指向特定消费者的"标识性信息"(如姓名、身份证号、手机号、收货地址)，也包括间接关联身份的"行为性信息"(如浏览历史、搜索记录、消费偏好、支付习惯)。需注意的是，"匿名化处理"是排除个人信息范畴的关键——若商家通过技术手段去除信息的可识别性(如将消费记录中的姓名、手机号替换为随机代码)，则该信息不再受《个人信息保护法》规制[1]。

2.2. 电子商务中个人信息的核心特征

1. 易得性：交易依赖下的信息获取便利化

电子商务的远程交易属性决定了消费者需提交个人信息以完成流程——注册账号时需提供手机号，下单时需填写收货地址，支付时需绑定银行卡信息。这种“信息换服务”的模式，使电商经营者能够在注册、浏览、下单、售后等全环节低成本收集信息，形成“被动式信息获取”优势。例如，消费者若拒绝电商平台“获取地理位置信息”的请求，可能无法使用“附近门店配送”功能；若不授权访问通讯录，则无法参与“邀请好友返现”活动，这种交易依赖导致个人信息收集具有天然的易得性[2]。

2. 可识别性：直接与间接关联的身份锁定

个人信息的可识别性分为“直接识别”与“间接识别”两类。直接识别是通过单一信息即可锁定主体，如姓名 + 身份证号、手机号等，这类信息在电商实名认证(如开通支付功能)中较为常见；间接识别则需通过多维度信息综合判断，例如通过消费者的浏览记录(如多次查看母婴用品)、消费频次(每月购买宠物食品)、收货地址(某小区)等数据，可间接推断其身份特征。随着大数据技术的发展，间接识别的精度不断提升，甚至可通过“碎片化信息拼接”还原消费者的完整画像，进一步放大了信息泄露的风险。

3. 双重属性：人身权与财产权的融合

电子商务中的个人信息兼具人身属性与财产属性。人身属性体现在信息与消费者人格尊严直接关联——如身份证号、生物识别信息的泄露可能导致身份冒用，侵犯消费者的人格权；财产属性则源于信息的商业价值，商家可通过分析信息实现精准营销，甚至将信息作为“商品”交易，形成产业链式的利益变现。例如，部分电商平台将消费者的消费等级、还款记录共享给金融机构，用于信贷额度评估。

3. 电子商务中个人信息受侵害的主要形态

3.1. 非法收集：超范围与诱导式收集并存

非法收集是电商领域个人信息侵害的“源头问题”，主要表现为“超范围收集”与“诱导式收集”两类行为。一方面，部分电商平台突破“必要原则”，收集与交易无关的信息——如购物 APP 要求访问手机通讯录、相册，外卖平台获取用户的健康数据，这些信息与商品销售、服务提供无直接关联，却被强制纳入收集范围。另一方面，诱导式收集通过“格式条款绑架”剥夺消费者选择权：平台将隐私政策与服务协议捆绑，消费者若不勾选“同意全部条款”，则无法使用核心功能。据统计，我国五款下载量过亿的电商 APP，平均每款需用户“阅读并同意”的协议内容约 2.7 万字，冗长复杂的法律术语使消费者难以真正理解权利义务，“同意”沦为形式化流程[3]。

从实践来看，电商平台的信息收集贯穿交易全周期：注册阶段收集基本身份信息，浏览阶段跟踪行为数据，支付阶段获取金融账户信息，售后阶段留存评价与投诉记录。这种“全环节收集”使消费者的信息被“碎片化切割”，但平台未明确告知各环节收集信息的用途，进一步加剧了非法收集的隐蔽性。

3.2. 非法销售：产业链式的信息利益变现

个人信息的商业价值催生了非法销售产业链，表现为“商家－中间商－下游使用者”的多层级流转。在电商领域，非法销售的典型场景包括：书籍电商将学生的购书记录、学校信息打包卖给培训机构，用于精准推销课程；母婴平台将孕妇的预产期、消费偏好转卖给奶粉品牌商，获取推广分成；家居电商将新房业主的地址、购房面积出售给装修公司，促成线下营销。更严重的是，部分不法分子通过黑客攻击电商平台数据库，批量窃取用户信息后，在暗网以“数据包”形式出售，形成“盗取－销售－滥用”的黑色产业链。

3.3. 非法利用：共享与侵扰式使用的双重风险

非法利用是个人信息侵害的“终端环节”，主要包括“未经授权共享”与“侵扰式使用”两类情形。

1. 未经授权共享：部分电商平台在未告知消费者的情况下，将信息与第三方机构共享——如与金融机构共享用户的支付记录，用于信用评估；与社交平台共享浏览记录，用于定向广告投放。这种共享缺乏明确的法律规制，消费者既无法知晓信息流向，也无法拒绝不必要的共享行为。例如，某电商平台与短视频 APP 合作，将用户在电商平台的“运动鞋浏览记录”同步至短视频平台，导致用户频繁收到运动鞋广告，引发隐私投诉。

2. 侵扰式使用：分为“推销式侵扰”与“报复式侵扰”。前者表现为商家基于收集的信息发送垃圾广告，如短信、邮件、APP 推送等，不仅占用消费者的时间与网络资源，还可能泄露信息用途；后者则是商家对“差评用户”的恶意报复——部分电商平台通过消费者预留的手机号、地址，实施骚扰，甚至威胁恐吓，这种行为既侵犯个人信息权益，也扰乱消费者的正常生活。

4. 电子商务中个人信息保护的现实困境

4.1. 法律体系：框架虽存但细则缺位，跨境规制不足

我国已形成以《个人信息保护法》《电子商务法》《网络安全法》为核心的法律框架，但实践中仍存在两大问题：

1. 配套细则缺失：《个人信息保护法》虽规定了“告知–同意”“数据最小化”等原则，但未出台具体实施细则——如“超范围收集”的界定标准、“匿名化处理”的技术规范等均不明确，导致执法机关在处理侵权案件时缺乏统一依据[1]。例如，某电商平台收集用户的“设备 MAC 地址”，执法机关难以判断该行为是否违反“必要原则”，最终只能以“警示整改”收场[4]。

2. 法律适用冲突：不同法律法规的适用范围存在交叉与矛盾——《电子商务法》侧重电商平台的义务规制，《个人信息保护法》强调信息处理者的责任，《网络安全法》聚焦数据安全，但三者在“跨境数据传输”“第三方责任”等条款上衔接不足。例如，《个人信息保护法》要求跨境传输个人信息需“确保接收国保护水平足够”，但未明确“足够保护水平”的评估标准；《电子商务法》仅规定平台需“采取技术措施保护信息”，却未提及具体技术要求[5]。

4.2. 行业层面：自律机制薄弱，技术防护不足

1. 行业自律组织缺位：我国电商行业的自律机制仍处于初级阶段，多数自律规范由行业协会或头部企业自行制定，缺乏强制性与普遍性。例如，中国电子商务协会曾发布《电子商务个人信息保护指南》，但该指南仅为“倡议性文件”，未规定违反后的惩戒措施，多数中小电商平台未落实指南要求。此外，跨境电商领域缺乏“跨国自律协作”，国际电商平台的信息保护标准与我国要求存在差异，却无统一的自律规则约束。

2. 技术防护投入不足：部分电商平台为降低成本，未采取足够的安全措施——如使用弱加密算法存储用户密码，未建立数据访问权限分级制度，导致数据库易被黑客攻击。2023 年某跨境电商平台发生数据泄露事件，约 500 万用户的姓名、手机号、支付记录被窃取，经查发现该平台未对敏感数据进行加密处理，且员工访问数据无需二次验证[2]。

4.3. 消费者层面：维权成本高，权利意识薄弱

1. 维权成本高于收益：消费者若遭遇信息侵害，需面临“举证难、周期长、费用高”的三重困境。一方面，信息侵权具有隐蔽性——消费者难以证明信息是被某电商平台泄露；另一方面，诉讼成本显著

高于收益——普通信息侵权案件的律师费、诉讼费约 5000~10,000 元，而消费者获得的赔偿通常仅为数百元，甚至“赢了官司输了钱”。

2. 权利意识薄弱：多数消费者对个人信息的法律权利认知不足——如不清楚《个人信息保护法》赋予的“访问权”、“删除权”，也不了解如何向网信部门、消费者协会投诉。此外，“同意疲劳”导致消费者对隐私政策“习惯性勾选”，既不阅读条款内容，也不关注信息用途，进一步弱化了权利保护意识。

5. 电子商务中个人信息保护的完善路径

5.1. 健全法律体系，统一适用规则

1. 出台配套实施细则：针对《个人信息保护法》《电子商务法》的模糊条款，制定专项细则——明确“超范围收集”的判断标准，规范“匿名化处理”的技术要求(如符合国家《个人信息匿名化指南》)，细化“公益诉讼”的启动条件。例如，可参考欧盟 GDPR 的“数据保护影响评估”制度，要求电商平台收集敏感信息前，需向网信部门提交评估报告，经审核通过后方可实施[6]。

2. 统一法律适用规则：梳理《个人信息保护法》《电子商务法》《网络安全法》的交叉条款，建立“优先适用”机制——如跨境数据传输问题优先适用《个人信息保护法》，电商平台的信息披露义务优先适用《电子商务法》，数据安全技术要求优先适用《网络安全法》。同时，制定“电商个人信息保护司法解释”，明确司法实践中的争议问题(如“侵扰式使用”的赔偿标准、“第三方共享”的举证责任分配)。

5.2. 强化行业自律：完善机制，提升技术防护

1. 构建多层次自律体系：由国家网信部门牵头，联合中国电子商务协会、头部电商企业，制定《电子商务个人信息保护行业标准》，明确平台的信息收集、存储、共享、删除等全流程义务[1]。同时，建立“行业自律惩戒机制”——对违反标准的平台，采取“警告、公示、暂停会员资格”等措施；情节严重的，移交执法机关处理。

2. 提升技术防护水平：推动电商平台落实“隐私设计”制度，在系统开发初期嵌入信息保护功能——如采用“数据最小化”技术、“动态授权”机制、“加密存储”措施。例如，可要求电商平台使用“差分隐私”技术，在分析用户行为数据时，加入噪声干扰，避免还原个体信息；同时，建立“数据泄露应急响应机制”，平台发生泄露事件后，需在 24 小时内通知用户与网信部门，并采取补救措施。

5.3. 优化维权机制：降低成本，强化权利保障

1. 推广公益诉讼与集团诉讼：落实《个人信息保护法》第七十条，鼓励检察院、消费者协会针对“大规模信息侵权”提起公益诉讼，代表消费者主张赔偿。例如，某电商平台泄露 10 万用户信息，消费者代表可提起集团诉讼，无需 10 万用户分别起诉，大幅降低维权成本。

2. 降低维权成本与举证难度：建立“电商信息侵权法律援助机制”，由政府补贴律师费，为消费者提供免费法律咨询与代理服务。同时，实行“举证责任倒置”——若消费者主张平台侵害其信息权益，平台需证明自身无过错，无法证明的则承担侵权责任。例如，消费者指控平台超范围收集信息，平台需提供“信息收集必要性说明”，否则视为侵权。

5.4. 提升消费者意识：加强教育，优化权利工具

1. 开展普法宣传：由网信部门、消费者协会联合电商平台，开展“个人信息保护宣传月”活动——通过短视频、漫画等形式，普及《个人信息保护法》的核心权利，讲解“如何识别非法收集行为”“如何投诉维权”。例如，可在电商 APP 首页设置“信息保护小课堂”，用户首次登录时强制观看 3 分钟普法

视频。

2. 优化“同意”机制：要求电商平台将隐私政策“通俗化、碎片化”——采用“分层告知”模式，核心条款用加粗字体突出，非核心条款可折叠；同时，提供“逐项同意”选项，允许消费者自主选择授权范围。例如，平台不得将“同意收集地址”与“同意收集通讯录”捆绑，需分开勾选。

6. 结语

电子商务中个人信息保护是数字经济发展的“必答题”，既关乎消费者的人格尊严与财产安全，也影响电商行业的可持续发展。当前，我国已构建个人信息保护的基础法律框架，但实践中仍面临法律细则缺位、行业自律薄弱、消费者维权困难等挑战。未来需通过“法律完善–行业自律–消费者赋能”的多维度协同，细化规则、降低成本，形成“事前预防–事中监管–事后救济”的全链条保护体系。个人信息保护“不可能一蹴而就，需要社会各方力量在较长时期内共同努力”。唯有持续优化保护机制，才能平衡电商发展与信息安全，为数字经济注入持久动力。

参考文献

[1] 廖文勇. 电子商务领域消费者个人信息保护对策分析[J]. 中国商论, 2023(11): 44-46.

[2] 郝芯. 电子商务时代大数据应用与个人信息保护的规范与实施对策[J]. 山西省政法管理干部学院学报, 2023(4): 89-92.

[3] 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.

[4] 李兴鹏. 跨境电商中个人信息保护的制度构建与完善——评《跨境电子商务法律问题研究》[J]. 出版广角, 2022(12): 89-91.

[5] 吴烨. 数字营商环境: 中国问题及法治路径[J]. 北方法学, 2024(2): 34-47.

[6] 欧盟. 通用数据保护条例(GDPR) [Z]. 2018.