

电子商务中消费者个人信息保护的 法律问题研究

张馨丹

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年9月15日; 录用日期: 2025年9月28日; 发布日期: 2025年10月28日

摘要

本文以电子商务中消费者个人信息保护为研究对象, 结合文献研究、规范分析与案例分析方法, 系统梳理我国以《个人信息保护法》为核心的多层次法律保护体系, 指出当前存在的立法界定模糊、法律衔接不畅、侵权责任可操作性不足, 监管权责不清、手段滞后、行业自律缺失, 以及消费者举证难、维权成本高、群体救济机制不健全等核心问题。在此基础上, 从立法(明确信息定义分类、强化法律衔接、细化侵权责任)、监管(厘清部门权责、创新技术监管、压实平台责任)、救济(推行举证倒置、完善公益诉讼、构建便捷维权渠道)三个维度提出针对性法律对策, 以期完善相关法律体系、平衡个人信息安全与数字经济发展提供理论参考。

关键词

电子商务, 消费者, 个人信息保护, 法律对策, 监管机制

Research on Legal Issues Concerning the Protection of Consumers' Personal Information in E-Commerce

Xindan Zhang

School of Law, Guizhou University, Guiyang Guizhou

Received: September 15, 2025; accepted: September 28, 2025; published: October 28, 2025

Abstract

This paper takes the protection of consumers' personal information in e-commerce as the research

object. Combining literature research, normative analysis and case study methods, it systematically sorts out China's multi-level legal protection system centered on the "Personal Information Protection Law", and points out the core problems currently existing, including vague legislative definition, poor legal connection, insufficient operability of tort liability, unclear regulatory powers and responsibilities, backward regulatory means, lack of industry self-discipline, as well as difficulties in burden of proof for consumers, high cost of rights protection, and inadequate collective relief mechanisms. On this basis, targeted legal countermeasures are proposed from three dimensions: legislation (clarifying the definition and classification of information, strengthening legal connection, and refining tort liability), supervision (clarifying departmental powers and responsibilities, innovating technical supervision, and consolidating platform responsibilities), and relief (implementing inversion of burden of proof, improving public interest litigation, and building convenient rights protection channels), aiming to provide theoretical reference for improving the relevant legal system and balancing personal information security and digital economic development.

Keywords

E-Commerce, Consumer, Personal Information Protection, Legal Countermeasures, Regulatory Mechanism

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

1.1. 研究背景与研究意义

在互联网技术深度渗透的当下，电子商务已成为驱动我国经济发展的核心引擎，并深刻重塑了大众消费模式。据最新数据显示，截至 2023 年 6 月，我国网络购物用户规模达 8.84 亿，占网民总数的 82.0%¹，网络购物已从“可选方式”转变为“生活必需”。而电子商务的便捷性高度依赖消费者个人信息的支撑，姓名、地址、支付信息、浏览偏好等数据不仅是平台优化服务、精准营销的核心资源，更承载着消费者的财产权益。

然而，电子商务的虚拟性、开放性与数据价值的攀升，使消费者个人信息安全面临严峻挑战。一方面，信息泄露与滥用事件频发：有大型电商平台过度搜集信息、第三方服务商违规流转数据等问题，甚至工信部 2021 年 4 月 6 日公布的《关于下架侵害用户权益 APP 名单的通报》中，136 家侵害用户权益 APP，有 53 款因拒不整改被强制下架，此类行为直接导致消费者遭遇诈骗、骚扰等损失，更冲击了行业信誉。另一方面，保护体系存在明显短板：尽管我国已形成以《个人信息保护法》为核心，《网络安全法》《民法典》《未成年人网络保护条例》等为支撑的法律框架，但法规对跨境数据传输、第三方处理者责任等新场景界定模糊，监管职责划分不清晰，加之消费者防护意识薄弱、易随意同意隐私协议，导致信息泄露后维权困难。

在此背景下，研究电子商务中消费者个人信息保护具有重要现实意义与理论价值。实践层面，通过明确保护困境、优化立法路径、厘清各方责任，既能为消费者权益提供坚实保障，也能规范行业发展秩序，营造可信的电商环境；理论层面，以法制构建为视角界定信息保护边界，可弥补现有研究对网购场

¹数据来源：第 52 次《中国互联网络发展状况统计报告》。

景特殊性的关注不足，为完善我国个人信息保护法律体系提供针对性参考，助力数字经济健康可持续发展。

1.2. 国内外研究现状

1.2.1. 国内研究现状

国内学界对电子商务中消费者个人信息保护的研究随行业发展与立法进程逐步深化。从研究脉络看，2012年前相关成果较为有限，2012年后因电子商务规模扩张及《网络安全法》《电子商务法》等立法推进，研究数量显著增长，2019年达到峰值。

研究内容主要集中于四方面：其一，个人信息法律属性与保护基础理论。学者围绕个人信息权性质形成多元观点，张新宝[1] (2018)提出区分敏感与一般信息分类保护，任龙龙[2] (2017)则将其界定为“框架性权利”以兼顾人格与财产价值；其二，电子商务领域信息侵权的具体形态。罗力[3] (2012)、何培育、王潇睿[4] (2017)等指出，平台过度搜集、二次加工、非法售卖信息及第三方中介违规处理是主要侵权形式，韩迎春[5] (2019)强调平台责任是保护核心；其三，保护路径的探索。郑宁[6] (2012)建议设立专门行政监管机构，于志刚[7] (2017)主张强化刑法保护，朱新力、周许阳[8] (2018)提出构建全国统一数据监测平台，姜素红、张可[9] (2018)等则呼吁出台专门立法明确权利义务；其四，立法实践与理论适配性讨论。针对《民法典》《个人信息保护法》的实施，学界就“个人信息保护究竟是权利还是权益”“现有法规对跨境数据、第三方处理等新场景的规制不足”等问题展开争议，同时普遍认为当前研究存在实证案例缺乏、制度设计与监管机制研究深度不足等局限。

1.2.2. 国外研究现状

国外因信息技术与电子商务起步较早，相关研究更为系统，形成了与本土立法实践紧密结合的理论体系。

美国学界主流观点将个人信息纳入隐私权范畴，帕克[10] (2012)认为，公民受教育程度和对隐私权的关注度成正相关，公民对隐私权的关注会促进其对隐私权保护采取具体的行动；日本学者聚焦法规的动态适配性，研究集中于《个人信息保护法》修订后对电商平台信息收集边界、跨境传输规则的完善，主张“分级分类保护”与行业特殊规范结合；韩国学界以严格立法为研究基础，围绕《个人信息保护法》《信息通信网络利用促进及信息保护法》等“数据三法”，探讨政府专门监管机构与平台责任的衔接，强调技术合规与法律规制的协同。此外，国外学者普遍注重实证研究，通过企业调研、案例分析验证保护机制的可行性，为立法修订提供支撑。

2. 电子商务中消费者个人信息保护的立法现状

2.1. 立法沿革

随着数字化时代的发展，我国在电子商务消费者个人信息保护立法方面不断探索前进。2006年，全国人大代表张学东提出制定个人信息保护法的建议，标志着我国开始关注个人信息安全问题。2009年，《刑法修正案(七)》首次将侵犯公民个人信息的行为纳入刑事制裁范围，同年的《侵权责任法》明确了个人信息的民事权益。

2012年，全国人大常委会审议通过《关于加强网络信息保护的決定》，为网络环境下的个人信息保护奠定基本规范。2013年修订的《消费者权益保护法》明确将个人信息保护纳入消费者权益。2015年至2018年间，《刑法修正案(九)》《网络安全法》和《电子商务法》相继颁布实施，进一步完善了个人信息保护的法律法规体系。2021年，《个人信息保护法》正式出台，标志着我国个人信息保护进入新阶段，为电子商务消费者个人信息保护提供了更全面、系统的法律保障。

2.2. 立法结构

我国已建立起一套涵盖宪法、法律、司法解释、行政法规、部门规章以及其他相关文件与标准的多层次个人信息保护法律体系。从立法层级看,随着法律效力层级降低,关于个人信息保护的立法规定由宏观向微观过渡,保护措施也日益具体化和细致化。

宪法虽未直接明确个人信息保护措施,但通过保护通信秘密体现了对个人信息保护的理念,为其他法律提供了原则性基础。《民法典》在明确了个人信息的定义、处理原则和权利内容,为个人信息保护提供了民事法律基础。《个人信息保护法》则在民法典基础上,对个人信息保护进行了更为细化和系统的规定,详细规定了个人信息的收集、公开、删除等规则以及处理者的权利与义务、法律责任等。《网络安全法》和《电子商务法》在个人信息保护方面提供了更具体的操作性规定,行政法规和部门规章则针对具体行业和领域进行了更细致的规范。

2.3. 现有立法规定。

2.3.1. 法律层面

在民事立法领域,针对网购消费者个人信息的保护,实施差异化的保护措施是至关重要的。我国《个人信息保护法》已经对个人信息进行了分类,明确划分为一般个人信息和敏感个人信息两大类^[11]。

《民法典》第 111 条承认了公民的个人信息权益,第 1034 条界定了个人信息范围,第 1035 条明确了收集、处理个人信息的原则。《消费者权益保护法》第 14、29、50、56 条对消费者个人信息保护作出规定,包括消费者个人信息受保护的权利、经营者不得擅自收集使用、保密义务以及侵权责任的承担等。

《电子商务法》第 23 条、24 条、25 条、79 条等规定了电子商务经营者对消费者个人信息的保护义务,如设置灵活的退出和修改机制、防范信息泄露等。《个人信息保护法》则全面系统地规定了个人信息处理的各个环节,强化了对电子商务消费者个人信息的保护。

2.3.2. 行政法规和部门规章层面

2013 年修订的《电信和互联网用户个人信息保护规定》,规定了网络服务提供者处理用户信息的相关要求。这些行政法规和部门规章进一步细化了电子商务消费者个人信息保护的具体措施,增强了法律的可操作性。

3. 电子商务中消费者个人信息保护存在的法律问题

3.1. 立法层面:制度设计存在缺陷与衔接不畅

3.1.1. 个人信息界定与分类保护体系不完善

随着科学技术的飞速进步,个人信息的重要性日益凸显,但是仍然存在肆意收集、盗取个人信息,这种情况日益严重,必须通过适当的法律措施加以限制^[12]。

尽管《个人信息保护法》明确将个人信息定义为“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息”,并区分了一般个人信息与敏感个人信息,但实践中仍存在界定模糊与分类粗糙的问题。一方面,匿名化处理后的信息是否仍属个人信息缺乏统一判断标准。随着大数据技术的发展,部分看似“匿名”的信息通过与其他公开数据关联分析,仍可精准识别特定消费者,如二手车历史车况信息结合车主身份信息即可锁定个人,但司法实践中对此类信息的定性仍存在争议。另一方面,敏感个人信息的分类标准不够细化。当前法律仅列举生物识别、宗教信仰等典型类别,但电子商务场景中高频涉及的消费偏好、支付习惯、物流地址等信息,其敏感程度因场景而异,却未被纳入差异化保护范畴,导致“一刀切”式保护难以适配复杂的电商数据处理需求。

3.1.2. 法律条款衔接存在漏洞与适用冲突

我国电子商务个人信息保护依赖《民法典》《个人信息保护法》《电子商务法》《网络安全法》等多部法律法规协同规制，但各法律间存在条款重叠、权责交叉甚至冲突的问题。例如，《网络安全法》侧重网络运营者的安全保障义务，《电子商务法》聚焦电商经营者的信息处理规范，而《个人信息保护法》构建了统一保护框架，但三者对“信息共享”“第三方责任”的规定表述不一，导致实践中法律适用困惑。在某电商平台擅自向第三方共享消费者信息的案例中，监管部门既难以依据《网络安全法》认定“网络运营者责任”，也无法直接适用《电子商务法》界定“电商经营者义务”，最终因法律衔接模糊导致处罚滞后。此外，部门规章与上位法的协调不足，如《电信和互联网用户个人信息保护规定》中关于“信息删除权”的规定，与《个人信息保护法》的“撤回同意权”存在表述差异，进一步加剧了执法与司法的操作难度。

3.1.3. 侵权责任与赔偿机制缺乏可操作性

现有法律对电子商务个人信息侵权的责任规定较为原则，难以满足实践维权需求。一是赔偿标准不明确。法律仅规定“按照实际损失或侵权获利赔偿”，但电子商务中消费者因信息泄露遭受的骚扰、诈骗等间接损失难以量化，精神损害赔偿也需满足“严重后果”要件，导致多数案件仅能获得象征性赔偿。二是举证责任分配失衡。尽管《个人信息保护法》规定了部分举证责任倒置情形，但消费者仍需证明“侵权行为存在”“信息由被告处理”等基础事实，而电商平台掌握数据存储、处理的核心证据，消费者因技术壁垒难以获取日志记录、数据传输轨迹等关键材料，导致维权成功率不高。

3.2. 监管层面：监管体系与手段滞后于实践发展

3.2.1. 监管权责划分模糊与协同不足

当前电子商务个人信息保护形成了网信、市场监管、公安、工信等多部门共管的格局，但部门间权责边界不清，易出现“多头监管”或“监管空白”。网信部门负责统筹协调，但缺乏具体执法权；市场监管部门侧重电商经营行为监管，对技术层面的信息处理合规性难以判断；公安部门仅针对刑事犯罪介入，对一般侵权行为缺乏监管手段。此外，跨区域监管协同薄弱，电子商务的无边界性使得信息侵权常涉及多地区主体，但地方监管部门缺乏数据共享与联合执法机制，进一步降低了监管效率。

3.2.2. 监管手段难以适配技术发展需求

传统“人工检查 + 抽样调查”的监管模式，已无法应对电子商务中大数据、人工智能等技术带来的挑战。一方面，海量数据处理导致监管覆盖不足。电商平台日均处理上亿条消费者信息，监管部门难以通过人工方式全面监测数据收集、共享、分析的全流程，使得“算法推荐”“自动化决策”中的信息滥用行为难以被及时发现。另一方面，技术壁垒加剧监管难度。不法分子利用区块链匿名性、AI 深度伪造等技术实施信息侵权，其行为隐蔽性强、痕迹易消除，而监管部门缺乏专业的技术检测工具与人才，难以实现对侵权行为的精准溯源。

3.2.3. 行业自律机制缺失与平台责任虚化

电子商务行业尚未形成有效的自律体系，平台作为信息处理的核心主体，其自我监管责任落实不到位。一是隐私政策流于形式。多数电商平台的隐私政策采用冗长晦涩的格式条款，消费者被迫“一揽子同意”，无法真正行使知情权与选择权。二是平台对入驻商家的审核与监管不足。部分平台未严格审核商家的信息处理资质，对商家非法收集、出售消费者信息的行为缺乏常态化监测，导致侵权风险沿“平台 - 商家 - 第三方”链条扩散。三是行业标准不统一。目前缺乏针对电子商务场景的个人信息处理行业规范，各平台在数据加密、存储期限、共享边界等方面自行其是，进一步加剧了监管难度。网络平台作

为公共空间，还经常出现非法信息交易的情况，因此电商运营者应当发挥出守门员的作用，对相关运营者的行为进行审查和监督，避免出现“公地悲剧”[13]。

3.3. 救济层面：消费者维权面临多重障碍

3.3.1. 举证能力不足与证据获取困难

电子商务个人信息侵权的证据多由电商平台、商家等掌握，消费者因技术与信息不对称，面临“举证难”的困境。一是基础证据缺失。消费者难以获取平台的信息收集日志、数据传输记录、第三方合作协议等关键证据，无法证明侵权行为与损害后果之间的因果关系。二是电子证据易篡改。电商平台的后台数据可被轻易修改，且缺乏第三方存证机制，消费者即使获取部分证据，也难以保证其真实性与完整性。三是专业鉴定成本高。涉及算法侵权、数据泄露等技术问题时，消费者需委托专业机构进行鉴定，单次鉴定费用高达数千元，超出普通消费者的承受能力。

3.3.2. 维权成本高与救济效率低下

消费者维权需付出的时间、精力与经济成本，成为阻碍其维权的重要因素。一是时间成本高。消费者需经历“与平台协商-向监管部门投诉-提起诉讼”的多重流程，协商周期通常长达1~3个月，诉讼程序则需6个月以上，漫长的过程使多数消费者选择放弃。二是经济成本高。除鉴定费外，消费者聘请律师的费用通常在5000元以上，而胜诉后的赔偿金额往往不足以覆盖维权成本。三是救济渠道不畅。监管部门的投诉处理存在“响应慢、反馈差”的问题。

3.3.3. 公益诉讼与群体维权机制不健全

针对电子商务个人信息侵权的群体性、扩散性特点，现有公益诉讼机制未能充分发挥作用。一是公益诉讼适用范围有限。根据《消费者权益保护法》，只有“侵害众多消费者合法权益”的行为才可由消协提起公益诉讼，但实践中多数侵权行为表现为“小额多量”，难以达到“众多”的认定标准。二是公益诉讼启动门槛高。消协需收集大量消费者的授权与证据，且缺乏专业的技术与法律支持。三是群体诉讼机制不完善。我国尚未建立专门的集体诉讼制度，消费者需通过“代表人诉讼”维权，但代表人的选任、意见统一等程序复杂，难以适应电子商务侵权中受害者分散、人数众多的特点，无法形成维权合力。

4. 电子商务中消费者个人信息保护的法律对策

4.1. 完善立法体系：构建精细化、协同化的法律框架

4.1.1. 明确个人信息定义与分类保护标准

基于《个人信息保护法》“可识别性”核心定义，应采用“概括+列举+动态解释”的模式细化界定。在立法中明确列举电子商务场景下的典型个人信息类型，包括姓名、身份证号、生物识别信息等核心身份信息，以及购物记录、浏览轨迹、支付偏好等行为信息，同时通过概括条款涵盖“与已识别或可识别自然人相关的其他信息”，为新型个人信息(如算法画像数据、设备指纹信息)预留规制空间。

针对匿名化信息的认定难题，需制定统一的技术与法律双重标准：明确匿名化需达到“不可逆、不可关联”的技术要求，即通过脱敏处理后，即使结合其他公开数据也无法识别特定消费者；同时规定企业对匿名化处理的举证责任，要求其留存处理过程记录并接受第三方审计。此外，应进一步细化敏感个人信息的分类，将电子商务中的支付信息、物流地址、健康消费数据等纳入敏感范畴，明确其收集需获得“单独同意”，且禁止用于非必要的商业营销。

4.1.2. 强化法律间的协调与衔接机制

针对《网络安全法》《电子商务法》《个人信息保护法》等法律的适用冲突，需通过制定专项司法解

释或行政法规构建“上位法统领 + 特别法补充”的适用规则：在个人信息的收集、处理、跨境传输等全流程规制上，优先适用《个人信息保护法》的统一要求；涉及电商平台的网络安全防护义务，适用《网络安全法》的技术规范；针对电商经营者的信息披露、平台责任等具体经营行为，适用《电子商务法》的特别规定。

建立跨部门立法协调机制，由网信部门牵头，联合市场监管、工信、公安等部门定期开展立法评估，对法律条文的冲突点进行动态修订。例如，统一各法律中“个人信息泄露通知义务”的时限要求，明确电商平台需在发现泄露后 72 小时内通知消费者及监管部门，并同步提交应急处置方案。同时，在《电子商务法实施条例》中增设“个人信息保护专章”，细化平台对入驻商家的信息管理义务，形成法律、行政法规、部门规章的层级衔接。

4.1.3. 细化侵权责任与引入惩罚性赔偿

明确电子商务个人信息侵权的归责原则与责任构成：对于电商平台，适用“过错推定责任”，即若消费者能证明个人信息在平台控制期间泄露，平台需举证证明已履行安全保障义务(如数据加密、访问权限管理等)，否则推定其存在过错；对于第三方服务商(如物流、支付机构)，则适用“过错责任”，由消费者举证其存在侵权行为。

在赔偿标准上，区分直接损失与间接损失：直接损失(如诈骗导致的财产损失)按实际金额赔偿；间接损失(如骚扰电话造成的时间浪费、精神困扰)可参照当地人均收入标准或侵权持续时间确定赔偿金额。同时，引入惩罚性赔偿制度，规定若电商平台存在故意泄露、大规模出售个人信息等“情节严重”的侵权行为，赔偿金额可按实际损失的 1~5 倍计算，且最低不低于 5000 元。通过较高的赔偿数额来惩罚商家不法行为，这也是惩罚性赔偿的主要功能[14]。

4.2. 强化监管效能：创新监管模式与责任机制

4.2.1. 明确监管职责与跨部门协同机制

通过立法清晰划分各监管部门的权责边界：网信部门负责统筹协调个人信息保护工作，重点监管电商平台的数据合规与跨境传输；市场监管部门聚焦电商经营者的信息收集、使用行为，开展隐私政策合规性审查；公安部门负责打击非法获取、出售个人信息的刑事犯罪；工信部门则对电商 APP 的技术安全进行监管，查处违规收集权限的行为。

建立“常态化协同 + 专项联合执法”机制：设立跨部门联席会议，每月通报监管数据与案件线索；搭建全国统一的个人信息保护监管平台，实现各部门数据共享，如市场监管部门将平台违规线索实时推送至网信部门，由其依法责令整改。针对跨境电商信息监管难题，联合海关、外汇管理部门建立“数据跨境传输白名单”，对符合安全评估标准的平台简化审批流程，对违规平台实施跨境数据传输限制。在侵犯消费者个人信息案件发展初期，从被动消极的处置模式转变为内控监管机制，在事前杜绝案件的发生。从事前监督到事后维权形成对侵害消费者个人信息的行为形成范围全覆盖，达到个人信息的保护和合理利用的平衡[15]。

4.2.2. 运用技术手段提升监管精准度

构建“大数据 + 区块链 + 人工智能”的智慧监管体系：由网信部门牵头建立电子商务个人信息监测平台，实时抓取各平台的信息收集弹窗、隐私政策文本，通过 AI 算法识别“默认同意”“概括授权”等违规条款，自动向平台发送整改通知；利用大数据分析消费投诉数据，对高频侵权领域(如直播电商、社区团购)开展定向执法检查。

引入区块链技术实现信息全流程溯源，要求电商平台将个人信息的收集、使用、共享记录上链存证，

监管部门可通过区块链节点实时查询数据流向，一旦发生泄露，可快速定位责任主体。例如，在物流信息管理中，通过区块链对快递单信息进行加密处理，仅授权配送员临时查看，确保信息不被滥用。此外，建立“监管沙盒”机制，对电商平台的新技术应用(如 AI 个性化推荐)进行合规测试，提前防范算法侵权风险。

4.3. 优化救济路径：降低维权成本与强化权利保障

4.3.1. 推行举证责任倒置与证据开示制度

针对电子商务中消费者举证能力薄弱的问题，在《民事诉讼法司法解释》中增设“个人信息侵权举证责任倒置条款”：消费者只需证明其向电商平台提供过个人信息、存在信息被侵权的事实(如收到骚扰短信、遭遇精准诈骗)，即可推定平台存在过错；平台需举证证明其已履行信息保护义务(如数据加密、员工保密培训等)，否则需承担侵权责任。

建立电商平台证据开示义务，法院可依消费者申请，责令平台提交信息收集日志、数据传输记录、第三方合作协议等关键证据。参考“庞理鹏案”的司法实践，明确平台无正当理由拒绝提供证据的，推定其存在侵权行为。同时，由市场监管部门牵头建立“电子商务个人信息侵权证据库”，统一存储投诉处理记录、平台合规报告等材料，为消费者维权提供证据支持。

4.3.2. 完善公益诉讼与群体维权机制

扩大公益诉讼主体范围，依据《个人信息保护法》第 70 条，明确消费者协会、检察机关均可针对“侵害众多消费者个人信息权益”的行为提起公益诉讼，包括平台大规模泄露信息、普遍存在违规收集行为等情形。在诉讼请求中增设“消除影响”“责令平台整改”等非财产性诉求，如要求平台删除非法收集的消费者数据、重构信息保护系统。

建立“示范诉讼 + 小额群体诉讼”机制：对于案情相似的个人信息侵权案件，由法院选取典型案例先行审理，判决结果对后续案件具有参照效力；针对涉及人数众多但单案标的较小的纠纷，允许消费者协会代表群体提起诉讼，采用“默示加入、明示退出”的方式简化程序，降低维权成本。例如，某电商平台因算法漏洞导致百万用户信息泄露时，消协可代表消费者集体索赔，赔偿金按比例发放给受损用户。

4.3.3. 构建便捷化、多元化的维权渠道

优化“12315”平台与“全国个人信息投诉举报平台”的联动机制，实现投诉一键转办：消费者提交投诉后，系统根据侵权类型自动分流至对应监管部门，要求其在 15 个工作日内反馈处理进度，30 日内出具处理结果。同时，在电商平台显著位置设置“个人信息维权入口”，直接对接监管部门，减少维权环节。

推广在线纠纷解决机制(ODR)，由市场监管部门认证的第三方机构提供在线调解、仲裁服务：消费者与平台可通过视频调解、电子签章等方式快速解决纠纷，调解协议具有法律效力；对调解不成的，可直接申请仲裁，仲裁结果可向法院申请强制执行。此外，加强消费者权益保护组织与电商平台的常态化沟通，建立“投诉预警 - 平台整改 - 效果评估”的闭环机制，推动平台主动优化信息保护措施，从源头减少侵权纠纷。

5. 结论

随着数字经济的深度发展，电子商务已成为我国居民消费的核心载体，而消费者个人信息作为电商服务的基础资源，其安全保护不仅关乎个体财产权益，更直接影响数字市场的健康秩序。本文围绕电子商务中消费者个人信息保护的法律问题展开系统研究，通过梳理立法现状、剖析核心困境、借鉴实践经验，形成了对该领域的全面认知，并为制度完善提供了针对性路径。

在立法现状层面，我国已构建起以《个人信息保护法》为核心，《民法典》《电子商务法》《网络安

全法》为支撑,行政法规、部门规章为补充的多层次法律体系,实现了从“零散规制”到“系统保护”的转变。但实践中,立法仍存在三大核心缺陷:一是个人信息界定与分类模糊,匿名化信息认定标准缺失,电商场景下的敏感信息(如支付习惯、物流地址)未得到差异化保护;二是法律衔接存在漏洞,多部门法对“信息共享”“第三方责任”等条款表述不一,导致执法与司法适用困惑;三是侵权责任机制可操作性不足,赔偿标准不明确、举证责任分配失衡,难以满足消费者维权需求。

监管层面的滞后性进一步加剧了保护困境。一方面,网信、市场监管、公安等多部门权责划分不清,存在“多头监管”与“监管空白”并存的现象,跨区域协同机制薄弱;另一方面,传统监管手段难以适配大数据、人工智能等技术发展,对算法歧视、区块链匿名侵权等新型行为缺乏有效监测与溯源能力;同时,行业自律机制缺失,电商平台隐私政策流于形式、对入驻商家监管不足,导致平台责任虚化。

救济路径的不畅则直接削弱了消费者的维权动力。由于电商平台掌握信息与技术优势,消费者面临“举证难”“成本高”“渠道堵”的三重障碍:关键证据由平台控制、电子证据易篡改,专业鉴定成本超出普通消费者承受能力;维权流程冗长、经济成本与赔偿收益失衡,导致多数消费者选择放弃;公益诉讼适用范围有限、群体诉讼机制不完善,难以应对侵权行为的群体性与扩散性特点。

针对上述问题,本文提出“立法完善-监管强化-救济优化”的三维解决路径:在立法层面,需通过“概括+列举+动态解释”明确个人信息定义,构建法律协调机制,细化侵权责任并引入惩罚性赔偿;在监管层面,应厘清部门权责、建立跨部门协同机制,运用大数据、区块链、人工智能等技术创新监管手段,强化平台自律责任;在救济层面,推行举证责任倒置与证据开示制度,完善公益诉讼与群体维权机制,构建便捷化、多元化的维权渠道。

电子商务消费者个人信息保护是一项系统性工程,需立法、监管、司法、行业与消费者形成合力。未来,随着数字技术的持续迭代,还需关注算法透明度、跨境数据传输、未成年人信息保护等新议题,通过动态修订法律、创新监管模式、强化主体责任,最终实现“个人信息安全”与“数字经济发展”的平衡,为我国数字市场的高质量发展提供坚实的法律保障。

参考文献

- [1] 张新宝. “普遍免费+个别付费”: 个人信息保护的一个新思维[J]. 比较法研究, 2018(5): 1-15.
- [2] 任龙龙. 个人信息民法保护的理论基础[J]. 河北法学, 2017, 35(4): 181-192.
- [3] 罗力. 电子商务消费者个人信息安全保护研究[J]. 情报探索, 2012(11): 48-50.
- [4] 何培育, 王满睿. 我国大数据交易平台的现实困境及对策研究[J]. 现代情报, 2017, 37(8): 98-105+153.
- [5] 韩迎春. 网购消费者个人信息保护研究——基于电商经营者义务的角度[J]. 佳木斯大学社会科学学报, 2019, 37(3): 50-52+67.
- [6] 郑宁. 我国网络环境下个人信息的行政法保护[J]. 四川理工学院学报(社会科学版), 2012, 27(6): 50-54.
- [7] 于志刚. “公民个人信息”的权利属性与刑法保护思路[J]. 浙江社会科学, 2017(10): 4-14+155.
- [8] 朱新力, 周许阳. 大数据时代个人数据利用与保护的均衡——“资源准入模式”之提出[J]. 浙江大学学报(人文社会科学版), 2018, 48(1): 18-34.
- [9] 姜素红, 张可. 论网络购物消费者个人信息的立法保护[J]. 湘潭大学学报(哲学社会科学版), 2018, 42(6): 73-76.
- [10] 邓胜利, 王子叶. 国外在线隐私素养研究综述[J]. 数字图书馆论坛, 2018(9): 66-72.
- [11] 郭明龙. 论个人信息之商品化[J]. 法学论坛, 2012, 27(6): 108-114.
- [12] 杨红灿. 中国《消费者权益保护法》修改与消费者个人信息保护[J]. 工商行政管理, 2015(16): 41-42.
- [13] 刘权. 网络平台的公共性及其实现——以网购平台的法律规制为视角[J]. 法学研究, 2020, 42(2): 42-56.
- [14] 王利明. 惩罚性赔偿研究[J]. 中国社会科学, 2000(4): 114-115.
- [15] 江小涓, 黄颖轩. 数字时代的市场秩序、市场监管与平台治理[J]. 经济研究, 2021, 56(12): 20-28.