E-Commerce Letters 电子商务评论, 2025, 14(5), 2621-2631
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.1451567

Hans汉斯

电子商务领域消费者隐私保护的法律路径

田钱莉

贵州大学法学院，贵州 贵阳

收稿日期：2025年4月13日；录用日期：2025年4月27日；发布日期：2025年5月29日

摘 要

随着电子商务的迅猛发展，消费者在享受便捷购物体验的同时，其隐私面临严峻挑战。个人信息在收集、存储、使用和传输等环节存在诸多安全隐患，泄露事件频发。本文旨在深入剖析电子商务领域消费者隐私保护的法律现状，探讨其中存在的问题，并提出完善法律路径的建议，以平衡电子商务发展与消费者隐私保护的关系，切实维护消费者合法权益。通过对相关法律法规及典型案例的研究，揭示当前法律在适用范围、责任界定、监管机制等方面的不足，进而从立法完善、执法强化、司法救济优化等角度提出针对性的解决措施。

关键词

电子商务，消费者隐私，法律路径，个人信息保护

Legal Path of Consumer Privacy Protection in the Field of Electronic Commerce

Qianli Tian

School of Law, Guizhou University, Guiyang Guizhou

Received: Apr. 13th, 2025; accepted: Apr. 27th, 2025; published: May 29th, 2025

Abstract

With the rapid development of e-commerce, while consumers enjoy the convenience of online shopping, their privacy is facing severe challenges. There are numerous security risks in the collection, storage, use and transmission of personal information, and leakage incidents occur frequently. This article aims to deeply analyze the current legal situation of consumer privacy protection in the e-commerce field, explore the existing problems, and propose suggestions for improving the legal path to balance the development of e-commerce and the protection of consumer privacy, and effectively safeguard the legitimate rights and interests of consumers. Through the study of relevant laws

文章引用: 田钱莉. 电子商务领域消费者隐私保护的法律路径[J]. 电子商务评论, 2025, 14(5): 2621-2631.
DOI: 10.12677/ecl.2025.1451567

and regulations and typical cases, it reveals the deficiencies of the current law in terms of the scope of application, responsibility definition, and regulatory mechanisms, and then proposes targeted solutions from the perspectives of legislative improvement, law enforcement strengthening, and judicial relief optimization.

Keywords

E-Commerce, Consumer Privacy, Legal Path, Personal Information Protection

1. 引言

在全球数字化转型的浪潮中，电子商务已然成为推动经济增长的核心驱动力。据中国互联网络信息中心(CNNIC)统计，截至 2023 年，我国网络购物用户规模突破 9.8 亿，全年电子商务交易额达 48.6 万亿元，占社会消费品零售总额的 30%以上。但繁荣背后，消费者隐私泄露风险急剧攀升。消费者在电商平台购物需提供大量个人信息，这为电商精准营销、个性化服务带来便利，却也使消费者隐私面临前所未有的挑战。近年来，快递面单信息泄露、电商平台数据遭黑客攻击等隐私泄露事件频发，给消费者造成极大困扰，甚至威胁财产安全与人身安全。不断出现的隐私侵犯问题、网络犯罪、信息诈骗等表明日益突出的网络安全及数据安全问题[1]。如 2022 年某头部电商平台因技术漏洞致数百万用户数据外泄，涉及个人身份、交易记录及生物识别数据，引发社会广泛关注。[1]此类事件严重损害消费者权益，动摇公众对数字经济的信任基础。因此，加强电子商务领域消费者隐私保护法律研究，对维护消费者权益、增强消费者对电商信任、促进电商行业健康可持续发展，以及推动我国数字经济时代法治建设、顺应全球数据保护趋势，都具有极为重要的现实意义。

国外在消费者隐私保护法律研究方面起步较早。美国通过多部法律构建起行业自律与法律规制相结合的模式，欧盟以《通用数据保护条例》(GDPR)为核心，确立严格统一的数据保护规则。国内学者针对电子商务领域消费者隐私保护开展大量研究，从完善法律体系、强化监管机制、促进行业自律等多维度进行探讨。不过，在法律具体适用以及应对新兴技术带来的挑战等方面，仍有待深入研究。

为深入探究该领域问题，本文运用多种研究方法。通过文献研究法，梳理国内外相关法律法规和学术成果，全面了解研究现状；借助案例分析法，剖析典型隐私泄露案例，揭示法律实践中的问题；运用比较研究法，对比国内外法律制度，汲取有益经验。创新之处在于紧密结合最新的电子商务发展动态与技术应用，如大数据、人工智能在电商领域应用对隐私保护产生的影响，提出具有前瞻性与针对性的法律路径建议，以期为电子商务领域消费者隐私保护提供有益参考。

2. 电子商务环境下消费者隐私保护的现状

2.1. 隐私泄露的典型场景与危害

电子商务场景中，隐私泄露主要集中于以下环节：

1) 数据过度采集：平台通过用户协议“捆绑授权”获取非必要信息(如通讯录、位置信息)；

[1]最高人民检察院《某知名电商平台用户信息遭泄露！问题出在哪儿？|今晚九点半》一文，可在最高人民检察院官网 http://m.toutiao.com/group/7443407380550812179/?upstream_biz=doubao。

2) 第三方数据共享：商家与物流、支付机构间的数据交换缺乏透明度；

3) 算法滥用：基于用户画像的“大数据杀熟”与定向广告引发歧视性待遇；

4) 跨境数据风险：跨境电商平台的数据存储与传输面临管辖冲突，如 TikTok 美国用户数据争议。

此类问题导致消费者面临财产损失(如精准诈骗)、社会评价贬损(如数据黑产中的名誉攻击)乃至人身安全威胁(如住址信息泄露引发的恶性事件)。据中国消费者协会 2023 年报告，超 65%的受访者因隐私问题减少在线消费，直接制约行业增长。

2.2. 相关法律法规概述

在电子商务中，消费者个人信息保护备受各界关注，我国关于个人信息的保护也在进一步地加强和完善[2]。我国已构建起以《中华人民共和国民法典》《中华人民共和国个人信息保护法》《中华人民共和国电子商务法》为主干，其他相关法律法规为补充的消费者隐私保护法律体系。《民法典》明确了隐私权的民事权利地位，规定了侵害隐私权的民事责任；《个人信息保护法》全面规范个人信息处理活动，确立了个人信息处理的基本原则、个人权利以及信息处理者的义务；《电子商务法》则对电商经营者在个人信息收集、使用等方面提出了具体要求。这些法律为消费者隐私保护提供了基本框架，但在具体实施中仍存在诸多问题。例如，法律规定较为原则化，缺乏可操作性；对违法行为的处罚力度不足；消费者维权渠道不畅等。这些问题导致消费者隐私保护的实际效果不尽如人意，亟需进一步完善相关法律制度。

2.3. 法律规定的主要内容

1) 个人信息的收集与使用规则：规定电商经营者收集个人信息应遵循合法、正当、必要原则，明示收集目的、方式和范围，并经消费者同意。使用个人信息不得超出约定用途，且应采取安全保护措施。

2) 消费者的权利：赋予消费者知情权、决定权、查阅权、复制权、更正权、删除权等一系列权利，以保障消费者对个人信息的控制。

3) 电商经营者的义务：包括安全保障义务，采取技术和管理措施防止个人信息泄露、篡改、丢失；定期合规审计义务，确保个人信息处理活动符合法律规定；以及向消费者告知义务，及时通知消费者个人信息处理相关事项。

2.4. 电子商务领域消费者隐私保护的法律路径比较与启示

2.4.1. 欧盟：统一立法与严格问责

欧盟《通用数据保护条例》(GDPR)通过“长臂管辖”与高额处罚(最高全球营收 4%)构建全球标杆。其核心经验包括：数据主体权利细化：如被遗忘权、可携带权、反对自动化决策权；数据保护官(DPO)制度：强制大型企业设立独立监督岗位；跨境数据流动“充分性认定”：通过“欧盟–日本互认协议”等机制平衡安全与流通。然而，GDPR 的合规成本令中小企业不堪重负，2022 年欧洲初创企业因数据合规支出平均增长 23%，部分企业被迫退出市场。

2.4.2. 美国：行业自律与分散立法

美国采取“联邦 + 州 + 行业”多层监管模式，如加州《消费者隐私法案》(CCPA)赋予用户数据删除权，医疗领域《HIPAA》规范健康信息使用。其优势在于灵活性高，鼓励企业通过“隐私盾认证”等自律机制创新。但分散立法导致监管真空，如 Meta 因跨州数据政策差异多次被诉。

2.4.3. 新兴法域的创新实践

巴西《通用数据保护法》(LGPD)：引入“数据保护影响评估”(DPIA)制度，要求企业在高风险数据

处理前进行系统性风险评估；印度《数字个人数据保护法案》：设立数据信托机构，代表用户行使数据权利；新加坡“可验证计算”试点：政府资助企业研发隐私增强技术(PETs)，降低法律执行成本。

综上可见，在消费者隐私保护方面，欧盟和美国代表了两种不同的法律路径。欧盟采取统一立法模式，制定了《通用数据保护条例》(GDPR)，为个人数据保护设定了严格的标准和全面的规则。GDPR 强调数据主体的权利，要求数据控制者承担更多责任，并对违法行为规定了高额罚款。相比之下，美国采取了分散立法模式，通过行业自律和特定领域的法律来保护消费者隐私，如《儿童在线隐私保护法》《健康保险可携性和责任法案》等。这两种法律路径各有优劣。欧盟的统一立法模式提供了全面、统一的保护标准，有利于跨境数据流动和执法协调，但可能增加企业合规成本。美国的分散立法模式更具灵活性，能够针对不同领域的特点制定相应规则，但可能导致保护标准不统一，存在监管漏洞。此外，巴西、新加坡等新兴法域国家在这方面也进行了一些创新和尝试。我国在构建消费者隐私保护法律体系时，可以借鉴上述模式的经验，采取“混合模式”：在顶层设计上借鉴欧盟的统一性原则，制定《个人信息保护法实施条例》细化规则；在行业层面参考美国灵活性，针对电商、金融、医疗等领域出台专门指引；同时通过“一带一路”数据合作倡议，推动区域性标准互认。

3. 电子商务领域消费者隐私保护存在的问题

3.1. 法律体系不完善

3.1.1. 法律法规之间存在冲突与空白

在电子商务领域消费者隐私保护的法律体系中，现存法律法规之间存在显著的冲突与空白问题[3]。从不同法律法规对个人信息定义的差异来看，《中华人民共和国民法典》第一千零三十四条规定，个人信息是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的各种信息。而《网络安全法》则更侧重于从网络运营者收集、使用个人信息的角度进行规范，对个人信息的界定与《民法典》存在细微差别。这种不一致导致在具体法律适用场景中，对于某一信息是否属于受保护的个人信息，不同执法者或司法人员可能产生理解偏差，进而引发法律适用的混乱。

在保护范围方面，不同法律也各有侧重。例如，《消费者权益保护法》主要聚焦于消费者在消费过程中所涉及的个人信息保护，其保护范围围绕传统消费行为展开。然而，随着电子商务模式的不断创新，诸如社交电商、直播电商等新兴业态不断涌现，消费者在这些新型电商场景下产生的个人信息，在《消费者权益保护法》中难以找到明确对应的保护范畴，而其他相关法律也未对此进行全面且清晰的覆盖，使得法律适用时对于新兴电商场景下个人信息保护范围的界定模糊不清。

责任认定同样存在诸多分歧。《电子商务法》规定了电子商务经营者对消费者个人信息的保护义务，但在责任认定方面，与《民法典》侵权责任编等法律存在衔接不畅的问题。当发生消费者隐私泄露事件时，对于电子商务平台经营者、平台内经营者以及第三方服务提供者之间责任的划分，不同法律规定存在不一致，使得在司法实践中责任认定困难重重，消费者权益难以得到有效保障。

3.1.2. 缺乏统一的隐私保护标准

在电子商务领域消费者隐私保护进程中，缺乏统一的隐私保护标准成为一大突出难题。当前，我国法律体系虽对电商领域隐私保护有所着墨，但相关规定多为原则性表述，缺乏清晰且具体的量化指标，这在实际操作中引发诸多困境。

以《网络安全法》为例，其要求网络运营者收集、使用个人信息，应遵循合法、正当、必要的原则，并公开收集、使用规则，明示收集、使用信息的目的、方式和范围。然而，对于“合法、正当、必要”原则的界定，法律并未给出明确量化标准。在实践中，电商经营者难以精准判断自身收集消费者个人信息

的行为是否符合这些原则。例如，电商平台为向消费者推送个性化广告，收集消费者浏览历史、搜索记录等信息，从平台角度可能认为这是为提升用户体验的必要之举，但从消费者权益角度，这些信息收集行为是否真的必要、正当，缺乏可量化的衡量依据，电商经营者难以准确把握合规界限。

再看《电子商务法》，虽规定了电子商务经营者保护消费者个人信息的义务，强调应采取技术措施和其他必要措施保障信息安全 ，但对于技术措施和其他必要措施的具体程度、达到何种标准才算保障信息安全，并未给出量化细则。这使得电商经营者在落实隐私保护措施时，缺乏明确指引。一些中小电商企业可能因缺乏专业技术能力，难以判断自身所采取的简单加密措施是否足以满足法律要求的保障信息安全标准。

对于监管部门而言，缺乏量化的隐私保护标准同样增加了监管难度。在监督检查电商经营者隐私保护工作时，由于没有具体量化指标作为参照，监管人员难以准确评估电商经营者的合规情况。例如，在检查电商平台数据存储安全措施时，对于存储设备的安全防护等级、数据备份频率等关键指标，因无明确量化规定，监管部门无法确切判断平台是否达到了应有的隐私保护水平，导致监管工作缺乏精准度与有效性，难以切实维护消费者在电子商务领域的隐私权益。

3.2. 监管机制不健全

3.2.1. 监管主体职责不明确

在电子商务领域消费者隐私保护的监管体系中，监管主体职责不明确的问题十分突出。当下，电商行业的隐私保护工作涉及多个监管部门，其中包括网信部门、市场监管部门以及公安部门等。然而，目前相关法律法规对于这些部门在消费者隐私保护监管方面的职责划分不够精细，致使在实际监管过程中频繁出现监管重叠与监管空白的不良现象。

网信部门在理论上主要负责统筹协调网络安全工作和相关监督管理工作。但在电商消费者隐私保护领域，其职责边界并不清晰。例如，在监测电商平台是否存在非法收集、传输消费者隐私数据的网络行为时，网信部门的监测范围和权限没有与其他部门明确区分。这就可能导致在某些情况下，网信部门与市场监管部门同时针对电商平台的同一数据收集行为展开调查，出现监管重叠，不仅浪费行政资源，还可能给电商企业带来重复应对监管的负担。

市场监管部门承担着规范和维护市场秩序的重要职责，在电商领域，理应监管电商经营者的经营活动，其中包含对消费者隐私保护情况的监管。但由于职责界定模糊，在处理一些新兴的电商隐私侵权行为时，市场监管部门常与公安部门出现职责交叉不清的状况。以电商平台数据泄露引发的消费者隐私侵权案件为例，市场监管部门认为此类案件涉及违法犯罪行为，应主要由公安部门处理；而公安部门则认为在对电商平台日常经营监管方面，市场监管部门应承担主要责任，这种相互推诿的情况就产生了监管空白。

公安部门在打击网络违法犯罪活动、维护社会治安秩序方面发挥关键作用，在电商消费者隐私保护方面，本应负责处理涉及侵犯公民个人信息的犯罪行为。但由于与其他部门职责划分不明，在一些涉及电商平台隐私保护的非刑事违法案件中，公安部门介入的界限不明确。例如，对于电商平台存在的轻度违规收集消费者信息行为，虽未达到刑事犯罪标准，但可能侵犯消费者权益，此时公安部门与市场监管部门之间的职责划分不清晰，容易导致监管不到位，最终致使整体监管效率低下，无法及时、有效地保护消费者在电子商务活动中的隐私权益。

3.2.2. 监管手段落后

监管部门肩负着保障消费者个人信息安全的重任，然而，其现有的技术手段却难以跟上电商领域的发展步伐。以个人信息收集环节为例，电商平台利用先进的算法和数据分析技术，能够精准且海量地收

集消费者的浏览偏好、购买历史、地理位置等多维度信息。而监管部门缺乏与之匹配的监测技术，无法实时、准确地获取平台收集信息的具体范围、方式及目的，难以判断其收集行为是否遵循合法、正当、必要的原则。

在个人信息存储阶段，电商企业为追求高效存储与便捷调用，常采用分布式存储、云存储等技术。这些存储方式在提升数据处理能力的同时，也增加了数据泄露风险。监管部门由于技术手段相对落后，难以对存储系统的安全性进行全面、深入的检测，无法及时发现潜在的安全漏洞，难以确保消费者个人信息在存储过程中的保密性、完整性和可用性。

当涉及个人信息的使用与传输时，问题更为凸显。电商平台借助人工智能算法实现个性化推荐，在这一过程中，个人信息被频繁调用与分析。同时，数据在不同业务系统、合作伙伴及第三方服务提供商之间快速传输。监管部门现有的技术工具难以对这些动态的信息使用与传输行为进行实时跟踪与监控，无法及时察觉未经授权的数据使用、非法的数据共享以及可能存在的数据泄露事件。

此外，在应对新兴技术如区块链在电商供应链中的应用时，监管部门更是面临巨大挑战。区块链的去中心化特性使得数据分布于多个节点，传统的集中式监管技术手段难以对其进行有效监管。缺乏先进的技术手段，监管部门无法实现对个人信息全流程的实时动态监管，在保障消费者隐私安全方面陷入被动局面，无法有效应对电商领域复杂多变的技术环境所带来的隐私保护难题。

3.3. 责任追究困难

3.3.1. 侵权责任认定复杂

在电子商务领域的隐私侵权案件中，侵权责任认定的复杂性极大地阻碍了消费者合法权益的有效维护。

第一，因果关系的认定困难重重。消费者在主张个人信息权益受到侵害时，需要证明个人信息泄露与电商经营者行为之间存在直接因果关系。但在实际情况中，这一证明过程极为棘手。一方面，电商平台运营涉及众多复杂环节，消费者个人信息在收集、存储、传输、使用及共享的各个阶段，都可能面临被泄露的风险。例如，在信息收集阶段，电商平台可能通过多种渠道，如用户注册、浏览记录追踪、第三方数据合作等方式获取消费者信息。存储环节中，数据可能存于平台自身服务器或依托云服务提供商，传输过程又涉及内部系统流转以及与外部合作伙伴的数据交互。如此复杂的信息处理流程，使得消费者难以确定信息泄露究竟发生在哪一环节，更难以证明与电商经营者特定行为之间的必然联系。另一方面，信息泄露途径呈现多样化且隐蔽的特点。除了电商平台自身的技术漏洞、内部员工违规操作可能导致信息泄露外，还可能因黑客攻击、第三方服务提供商的疏忽等原因造成。这些外部因素的介入，进一步模糊了信息泄露与电商经营者行为之间的因果关系，导致消费者在举证时面临巨大挑战。

第二，过错认定标准不明确，为电商经营者推脱责任提供了可乘之机。在隐私侵权案件中，对于电商经营者过错的判断缺乏清晰、统一的标准。电商经营者常常利用这一漏洞，以各种理由推卸责任。例如，在面对因技术漏洞导致的信息泄露事件时，电商经营者可能声称已采取了行业内普遍认可的安全防护措施，对于此次技术漏洞的出现无法预见且已及时进行修复，不应承担过错责任。在涉及第三方数据合作引发的信息泄露问题上，电商经营者又可能将责任归咎于第三方，强调自身已对第三方进行了合理审查，无法对第三方后续的违规行为负责。此外，一些电商经营者还会以消费者自身操作不当，如设置简单密码、在不安全网络环境下登录等为由，试图减轻或免除自身责任。这种过错认定标准的模糊性，使得在司法实践中，法官对于电商经营者是否存在过错的判断存在较大自由裁量空间，消费者往往因难以证明电商经营者的过错，而无法获得应有的赔偿与救济，严重削弱了法律对消费者隐私权益的保护力度。

3.3.2. 赔偿范围和标准不明确

在电子商务领域，当消费者遭遇隐私泄露时，赔偿范围和标准的不明确严重损害了消费者权益。目前，针对此类情况的赔偿范围过度局限于直接经济损失。比如消费者因个人信息泄露，账户资金被盗刷，盗刷金额属于直接经济损失，可获赔偿。但在实际中，隐私泄露给消费者带来的远不止于此。精神层面，消费者因个人隐私曝光，可能陷入焦虑、不安，生活受到严重干扰，然而精神损害赔偿规定模糊，消费者很难就此获得合理补偿。从间接损失看，因个人信息泄露，消费者可能错过重要商业合作、求职机会，这类间接损失因缺乏明确赔偿规定，难以得到赔偿，致使消费者获赔难以弥补实际遭受的全部损失。

3.4. 消费者维权困境

3.4.1. 维权成本高

在电子商务领域，消费者一旦遭遇隐私泄露进行维权，往往会陷入维权成本高企的困境。从时间维度来看，消费者首先需要花费大量时间去收集证据。由于个人信息泄露的途径复杂且隐蔽，可能涉及电商平台的各个运营环节，消费者需仔细梳理自身在该平台的所有操作记录，包括注册信息、购物流程、接收的各类通知等，从中寻找信息泄露的蛛丝马迹。同时，还需联系相关平台客服获取数据使用说明、交易日志等资料，这一过程需反复沟通、等待，可能耗费数周甚至数月时间。

精力方面，消费者不仅要应对繁琐的证据收集工作，还需深入研究相关法律法规，了解自身权益以及维权流程。面对专业性极强的法律条文，非法律专业的消费者需付出巨大精力去学习、理解。在准备诉讼材料阶段，需逐字逐句撰写投诉信、整理证据清单，确保材料完整、准确，稍有差错便可能影响维权进程。

经济成本更是让许多消费者望而却步。聘请专业律师是维权的重要途径，但律师费用通常较高，对于普通消费者而言是一笔不小的开支。若案件涉及复杂技术问题，还可能需要聘请专家证人进行技术鉴定，这又进一步增加了经济负担。此外，参与诉讼过程中的交通费用、误工损失等也不容小觑。如此高昂的维权成本，使得众多消费者即便深知自身权益受损，也只能无奈放弃维权，这无疑助长了电商领域隐私侵权行为的滋生。

3.4.2. 举证难度大

在电子商务领域，消费者在隐私侵权纠纷中面临着极为严峻的举证难题。消费者天然处于信息劣势地位，这一状况极大地阻碍了其获取电商经营者侵权的关键证据。电商平台作为信息的掌控者，拥有复杂且封闭的信息处理系统，消费者仅能看到前端的界面操作，对于后端信息收集、存储、使用以及共享的具体流程和细节知之甚少。例如，消费者在注册电商平台时，虽同意了平台的隐私政策，但这些政策条款往往冗长晦涩，普通消费者很难完全理解其中关于个人信息处理的关键信息。而在实际运营中，电商平台利用先进的算法和技术手段，在消费者浏览商品、下单购买等日常操作过程中，悄然收集大量个人信息，包括浏览偏好、消费习惯、地理位置等多维度数据。这些数据的收集、存储和流转均在平台内部完成，消费者难以察觉，更无从获取相关记录作为侵权证据。

同时，电商平台与第三方合作频繁，消费者个人信息在不同主体之间的传输路径错综复杂。消费者在不知情的情况下，其信息可能已被共享给多个第三方服务提供商，用于精准营销、数据分析等目的。但由于信息的流转发生在平台与第三方的商业合作网络中，消费者既无法实时跟踪信息的流向，也难以获取涉及信息共享的合同、协议等关键证据材料。

更为棘手的是，当前法律在举证责任分配上，未能充分考量消费者所处的这种信息劣势地位。在传统的侵权纠纷中，通常遵循“谁主张，谁举证”的原则，要求消费者承担主要的举证责任来证明电商经营者存在侵权行为。然而，在电商隐私侵权案件中，这一原则对消费者极为不利。消费者不仅缺乏获取

证据的渠道和能力，而且面对专业性强、技术门槛高的电商运营系统，难以从复杂的技术架构和海量的数据处理流程中挖掘出有力的侵权证据。这无疑进一步加剧了消费者维权的难度，使得众多消费者即便遭受隐私侵权，也因无法有效举证而难以维护自身合法权益。

4. 完善电子商务领域消费者隐私保护的法律路径

4.1. 完善立法

4.1.1. 统一法律规范

现有涉及电子商务隐私保护的法律法规，分散于《网络安全法》《电子商务法》《消费者权益保护法》等多部法律之中。这些法律虽各有涉及，但在具体规定上存在诸多冲突。例如，对于个人信息定义，不同法律从不同侧重点出发，导致界定范围模糊不清。《网络安全法》侧重于网络运营者收集、使用个人信息方面的定义，而《消费者权益保护法》更多从消费者权益保障角度出发，两者在概念的外延与内涵上存在差异。这种不一致使得在实际应用中，电商经营者和执法者难以准确判断某一信息是否属于受保护的个人信息范畴。

在保护范围方面，各法律规定也不尽相同。《电子商务法》主要围绕电子商务经营活动中产生的消费者信息保护展开，而《网络安全法》涵盖了更广泛的网络运营场景下的个人信息保护，这就造成在一些新兴电商业务模式中，如社交电商、直播电商所涉及的消费者隐私保护，出现法律适用的模糊地带。

权利义务关系同样亟待明确。电商经营者、消费者以及第三方服务提供商在个人信息处理过程中的权利义务分配不清晰。电商经营者对于消费者个人信息的收集权限、使用目的以及存储期限缺乏明确界定；消费者对于自身信息被收集、使用的知情权、控制权以及获得有效救济的权利在现有法律中表述较为笼统；第三方服务提供商在获取、使用消费者信息时，与电商经营者和消费者之间的权利义务关系更是缺乏清晰规范。

因此，制定专门的电子商务隐私保护法，能够系统地整合现有法律法规，消除这些法律冲突。通过明确个人信息定义，精准划定保护范围，清晰界定各方权利义务关系以及严格规范法律责任，形成一个统一、协调且具有权威性的法律体系，为电子商务领域消费者隐私保护提供坚实的法律保障。

4.1.2. 细化隐私保护标准

在电子商务蓬勃发展的当下，制定详尽且切实可行的隐私保护技术标准和管理规范迫在眉睫。由于电商领域个人信息的处理环节极为复杂，从数据的收集、存储到使用和传输，每个阶段都存在隐私泄露风险，因此需要一系列明确标准加以规范。

在数据加密方面，应制定严格的数据加密标准。电商经营者收集的消费者姓名、身份证号、银行卡信息等敏感数据，在传输与存储过程中必须采用高强度加密算法。例如，强制要求使用行业领先的 AES (高级加密标准) 256 位加密算法，防止数据在传输过程中被窃取或篡改。对于不同敏感度的数据，要依据风险等级划分加密级别，像支付信息这类高敏感数据，需采用最高等级加密，并定期更新加密密钥，确保加密的时效性与安全性。

安全存储期限同样需要精准规范。电商经营者不应无限制地存储消费者个人信息，应根据信息的使用目的和必要性确定合理的存储期限。比如，消费者的浏览历史数据，若仅用于短期的个性化推荐，在推荐周期结束后的一定时间内(如 30 天)，应删除或匿名化处理；而涉及交易合同、售后保障等必要信息，可依据相关法律法规规定的最短保存期限(如《电子商务法》规定的商品和服务信息、交易信息保存时间自交易完成之日起不少于三年)进行存储。超过存储期限后，需通过安全可靠的方式彻底删除数据，避免数据长期留存带来的泄露风险。

访问控制要求也是关键一环。电商企业内部需建立严格的访问权限管理体系，对能够接触消费者个人信息的员工进行分级授权。只有经过专门授权的特定岗位人员，如数据管理员、客服主管等，才能在履行工作职责必要的范围内访问相关信息。同时，采用多因素身份验证机制，除密码外，还需结合指纹识别、短信验证码等方式，确保访问者身份真实可靠。在访问过程中，对操作行为进行全程记录，包括访问时间、访问内容、操作记录等，以便事后审计追踪，一旦发生信息泄露事件，能够迅速定位问题源头。

4.2. 强化监管

4.2.1. 明确监管主体职责

我国必须要去建立和完善独立的、专门从事消费者个人信息保护工作的组织[4]。为有效提升电子商务领域隐私保护监管效能，清晰界定各监管部门职责并构建协同机制至关重要。目前，电商隐私监管涉及网信、市场监管、公安等多部门，但职责边界模糊。应明确网信部门在统筹协调网络安全与信息管理层面的核心地位，全面规划电商隐私保护策略，搭建信息共享平台，整合各方资源。市场监管部门专注于规范市场经营行为，对电商平台个人信息收集、使用等环节进行日常巡查，监督平台是否依规公示隐私政策、有无超范围收集信息等。公安部门凭借执法权，全力打击侵犯消费者隐私的违法犯罪活动，如针对黑客攻击、非法售卖个人信息等行为展开专项行动。通过建立常态化协同监管机制，加强部门间信息共享，实现线索移送、联合执法等高效协作，凝聚强大监管合力，全方位筑牢电商隐私保护防线。

4.2.2. 创新监管方式

在电子商务领域，创新监管方式对强化消费者隐私保护极为关键。借助大数据、人工智能等前沿技术，构建智能化监管平台刻不容缓。该平台能对电商平台个人信息处理活动进行实时监测，运用大数据分析技术抓取海量数据，精准识别异常信息流动，如短期内大量个人信息被集中调取、传输至不明第三方等行为。依托人工智能算法，可对监测数据进行深度分析，实现风险预警，提前预判潜在隐私泄露风险。当风险值达到设定阈值，立即发出警报，为监管部门争取处置时间，达成精准监管。

与此同时，大力推行信用监管势在必行。将电商经营者的隐私保护情况全面纳入信用评价体系，详细记录平台信息收集合规性、泄露事件处理成效等指标。对隐私保护良好的企业给予信用加分，在政策扶持、业务拓展等方面予以倾斜；对违规者实施联合惩戒，如限制其参与政府采购、金融信贷，提高其市场准入门槛等，以此督促电商企业重视隐私保护，营造健康有序的电商环境。

4.3. 加强责任追究

4.3.1. 简化侵权责任认定

在电子商务隐私侵权案件中，当前侵权责任认定流程复杂，严重阻碍消费者维权，亟待简化。可采用过错推定原则，扭转消费者在举证方面的劣势。过往遵循“谁主张，谁举证”原则，消费者要证明电商经营者存在过错，需耗费大量精力。而实行过错推定后，直接推定电商经营者存在过错，其必须主动证明自身在个人信息保护方面已采取完备措施，如安全的数据存储体系、规范的员工操作流程等，以此自证无过错。同时，要清晰明确因果关系认定标准。以往消费者需证明个人信息泄露与电商经营者行为存在直接、必然联系，难度极大。今后，只要消费者能证实个人信息泄露与电商经营者存在一定关联，比如信息泄露时间与平台系统更新、数据共享操作时间相近，或泄露信息类型与平台收集信息范畴高度吻合等，即可初步认定因果关系成立。这一改变大幅减轻消费者举证负担，提升维权效率，有力保障消费者权益。

4.3.2. 明确赔偿范围和标准

在电子商务隐私侵权赔偿领域，明确且合理的赔偿范围与标准，对维护消费者权益意义重大。现行赔偿体系局限于直接经济损失，亟需完善。应扩大赔偿范围，将精神损害赔偿纳入其中。消费者因个人信息泄露，常面临骚扰电话、垃圾邮件轰炸，甚至个人隐私被曝光，精神备受折磨，理应获得精神损害赔偿。同时，间接损失赔偿也不容忽视，如因信息泄露，消费者错失商业合作机会、求职受阻，这类间接损失应得到合理补偿。为精准确定赔偿数额，需制定科学合理的赔偿标准。依据侵权情节，考量电商经营者侵权行为的主观恶意程度、信息泄露的规模及持续时间；结合损害后果，如消费者实际经济损失大小、精神受创程度等因素，综合判定赔偿数额。通过这样的方式，确保消费者所获赔偿能够充分弥补因隐私侵权遭受的各类损失，彰显法律对消费者权益的有力保护。

4.4. 优化消费者维权机制

4.4.1. 降低维权成本

为切实保障消费者在隐私维权方面的权益，降低其维权成本刻不容缓。建立专门的消费者隐私维权机构是关键举措。该机构配备专业法律团队，为消费者提供免费法律咨询，帮助其明晰自身权益以及维权途径，无论是解答电商平台隐私政策相关疑问，还是分析侵权行为性质，都能给予专业指导。同时，针对经济困难或缺乏法律知识的消费者，提供法律援助，全程协助其维权，包括收集证据、撰写法律文书、参与诉讼等。机构还设置调解服务，在尊重双方意愿基础上，高效化解纠纷，减少消费者时间与精力耗费。设立小额诉讼程序同样重要。对于因隐私侵权产生的小额纠纷，简化繁琐诉讼流程，免去复杂证据交换、冗长庭审环节，采用书面审理、线上开庭等便捷方式。缩短案件审理周期，快速作出裁决，大幅降低消费者在时间、经济上的维权成本，让消费者维权之路更为顺畅。

4.4.2. 完善举证责任分配

在电子商务隐私侵权案件中，完善举证责任分配对于保障消费者权益意义重大。当前消费者处于信息劣势，举证困难，实行举证责任倒置势在必行。让电商经营者承担主要举证责任，要求其提供详实证据，证明自身已构建合理安全措施，如展示完备的数据加密技术应用、规范的员工信息访问权限管理、定期的系统安全漏洞检测报告等，以证实未泄露消费者个人信息。与此同时，积极鼓励消费者借助现代技术手段提高举证能力。网络公证机构能对消费者在电商平台的操作过程、收到的可疑信息等进行公证，确保证据真实性与合法性。电子证据保全平台可帮助消费者及时固定聊天记录、页面截图、交易日志等关键证据，防止证据灭失或被篡改。通过这两种方式，消费者在维权时能更好地维护自身权益，推动案件公平公正解决。

5. 结论

电子商务领域消费者隐私保护是一个复杂而重要的问题，关系到消费者切身利益和电子商务行业的健康发展。当前我国虽已建立起一定的法律保护体系，但仍存在诸多问题。通过完善立法、强化监管、加强责任追究和优化维权机制等法律路径，可以有效加强消费者隐私保护。在未来的研究中，还需持续关注电子商务领域的新技术、新模式，不断完善法律制度，以适应不断变化的隐私保护需求，在数字经济时代实现消费者隐私保护与电子商务发展的良性互动[5]。

参考文献

[1] 孙畅. 数字经济背景下消费者隐私保护的经济分析[J]. 现代商业, 2024(13): 31-34.

[2] 祁震. 电子商务中消费者个人信息保护问题的调查及法律对策研究[J]. 网络安全技术与应用, 2022(4): 109-111.

[3] 马金. 电子商务环境下消费者个人信息的法律保护探究[J]. 中国市场, 2019(31): 185-186.

[4] 邵彪, 李正辉, 马梅兰. 大数据时代电子商务中消费者隐私保护问题及对策[J]. 网络安全技术与应用, 2023(9): 126-128.

[5] 唐卫玲. 网络购物中消费者个人信息的法律保护[J]. 河北企业, 2018(7): 156-157.