

电子商务个人信息保护的挑战及其纾解研究

周念九, 徐以超*

江苏大学法学院, 江苏 镇江

收稿日期: 2024年4月29日; 录用日期: 2024年5月24日; 发布日期: 2024年8月6日

摘要

随着“互联网+”战略的推进, 电子商务行业迅猛增长, 消费者个人信息成为了极为重要的资产。然而, 因为网络平台与商家对信息的商业利用, 消费者的隐私权保护遭遇了前所未有的风险。因此, 需要在厘清电子商务个人信息特殊性质的基础上, 探讨电子商务个人信息保护的现实挑战, 并从立法、监管、救济三个方面提出对应的纾解路径, 以促进电子商务行业的长期和健康发展。

关键词

电子商务, 消费者, 个人信息保护

Research on the Challenges and Solutions of Personal Information Protection in E-Commerce

Nianjiu Zhou, Yichao Xu*

Law School of Jiangsu University, Zhenjiang Jiangsu

Received: Apr. 29th, 2024; accepted: May 24th, 2024; published: Aug. 6th, 2024

Abstract

With the emergence of the new “Internet plus” format, the e-commerce industry has developed rapidly, in which consumer personal information plays an important role and becomes the most popular resource with the help of the rapid spread of the Internet. Especially in the field of e-commerce, due to the commercial value of personal information being seized by network platforms and operators, consumer personal information protection often faces severe chal-

*通讯作者。

lenges. There is still great room for progress in the legal efforts to protect consumer personal information rights, and it is urgent to promote institutional optimization governance with social forces. Therefore, it is necessary to clarify the practical challenges and relief paths of personal information protection in e-commerce, in order to help the long-term and healthy development of the e-commerce industry.

Keywords

E-Commerce, Consumers, Personal Information Protection

Copyright © 2024 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

电子商务的迅速发展与大数据技术在个人信息利用方面的应用密不可分。个人信息作为一种创新资源,与传统资源不同,其价值在使用过程中不会减损,反而可以通过技术整合及多次利用实现更大的经济效益。正因如此,不少电商平台和商家对个人信息的追求达到了近乎极端的程度,这种做法不仅可能侵犯个人的信息权利,还可能导致信息权益的多方面损害。在电子商务的环境下,个人信息的收集、处理、存储及使用等环节经常出现问题,如平台或商家的强制信息获取、过度挖掘和分析,以及信息泄露和非法销售等行为,这些问题不仅侵害了消费者的实际权益,也可能侵犯到他们的潜在权益。考虑到网络大数据的特性和平台与消费者间的力量不平等,每一次个人信息的侵权行为都可能影响广大用户,带来严重的后果。因此,如何迅速有效地处理电商消费者在个人信息法律保护方面的挑战,已成为一个急需解决的关键问题。

2. 电子商务个人信息概述

2.1. 电子商务个人信息的法律属性

尽管我国当前的网络消费者个人信息权保护制度未具体明确网络个人信息权的定义,但《中华人民共和国个人信息保护法》第四条对此已给出确切的定义,明确将个人定位为信息权的主体。在此背景下,消费者这一特定社会群体的个人信息,虽然源于一般个人信息,却具有其特殊性。这包括消费者在购买、使用产品或服务过程中所提供或产生的信息,这些信息能指向特定身份,核心在于其可识别性,即能否精确识别特定消费者。学术界普遍认可的“识别说”持有观点,个人信息是独一无二的。根据此观点,信息的主体应与个人信息相匹配,关键在于信息能否直接或间接地“识别”主体^[1]。网络消费者的个人信息多在消费或交易中产生,故在电子商务环境中应进一步扩展。科技的进步使得电子商务运营者能够获取消费者未直接意识到的有价值信息。然而,若仅依赖这些数据来识别消费者,可能引发认知局限和不完整性。因此,有必要进一步拓展消费者个人信息的内涵,并在必要时打破“可识别性”原则的限制。尽管“可识别性”广泛应用于电子商务之外,许多学者仍推崇“关联说”,即与消费者密切相关的信息。依据“识别说”和“关联说”,个人信息可以分为能够独立通过特定信息直接或间接识别某一消费者的两大类。因此,本文认为电子商务中消费者的个人信息指在电商平台购买商品或服务时产生的,与消费者密切相关的信息,这些信息能够直接或间接地识别消费者。

2.2. 电子商务个人信息保护的特殊性

虽然我国在保障消费者个人信息的法律体系逐渐完善,但由于电子商务的特点,例如其虚拟性、隐蔽性及信息不对称性,使得网络消费者与传统消费者在权益保护上存在显著差异。网络消费者的个人信息侵权事件仍时有发生,这加剧了他们的不安全感。在数字经济时代,个人信息保护显示出几个独特的特点:

第一,个人信息可识别性强。得益于互联网技术的迅猛发展,大数据和智能技术的应用能够迅速而准确地识别消费者的个人资料及其消费行为。这种高度的可识别性,虽然为消费者提供了高效的服务体验,同时也带来了巨大的隐私保护挑战。个人信息的高商业价值也驱使商家通过这些信息追求更高的经济利益[2]。

第二,个人信息侵犯可能性高。互联网的信息化和数据化特征导致个人信息在采集、应用和交易的过程中形成了完整的产业链。这不仅增加了信息泄露的风险,还使得一旦信息被上传至平台,个人信息的保护难度大增。随着技术的发展,消费者对自己信息的控制能力减弱,信息处理者能深入挖掘这些数据,对消费者的隐私安全构成威胁。

第三,个人信息侵权主体复杂。在电子商务领域,不仅有电商平台、商家,还涉及物流等多方。个人信息的收集和处理常被外包,使得追踪侵权源头变得复杂。侵犯个人信息的行为分散,多个环节可能共同导致侵权,这增加了追责的难度。

第四,个人信息商业价值高。消费者的个人信息已成为极具价值的数据资产,处理这些信息的人可能为了追求利润而冒险,忽视法律规定,威胁到消费者的安全。

3. 电子商务个人信息保护的现实挑战

3.1. 电子商务个人信息保护缺乏立法针对性

电商消费者个人信息保护在立法上的针对性不强主要体现在对电商消费者个人信息的权利实现规定缺乏可实现性。

第一,电子商务消费者的个人信息知情权未得到充分实施。尽管《个人信息保护法》第四十四条和《电子商务法》第十七条都明确规定了消费者的知情权,这些规定更多地是声明性的,它们强调消费者应享有知情权,且平台需确保这一权利,但如何具体实施这一权利却未详细说明。通常情况下,消费者在使用移动端或PC端访问电商平台前,平台会通过格式化条款通知消费者其个人信息将被收集。即便消费者仔细阅读了这些条款,也很难完全理解其个人信息的收集范围及方式,往往是为了获得使用平台的资格而草率同意。此外,消费者在网购时,他们可能注意到曾在其他应用中搜索的关键词,这些关键词会迅速出现在购物应用的首页推荐中。消费者对这种基于个人信息流转进行的精准推送方式并不了解。这可能导致实际使用个人信息的方式与之前的通知不一致,或消费者对此完全不知情,更严重的是,可能会导致个人信息泄露。

第二,电子商务消费者的个人信息删除权未得到充分执行。《个人信息保护法》实施后,增加了名为删除权的重要权利,该权利在法律的第四十七条中有明确规定,对保护电商消费者的个人信息至关重要。电商交易不同于传统的通讯或社交平台,它涉及线上到线下的完整交易链。一个网络交易可能涉及多个参与方,如平台、商家和快递运营商等。消费者提供的信息会在这些参与方之间流转、存储和使用。特别是快递运营商,由于快递的选择和更换通常由商家决定,每次更换都会导致消费者信息的再次流转。在这种复杂的信息流转过程中,消费者难以与每个参与方确认其个人信息的权利,与快递服务提供商的直接交流机会也少之又少。在这样的背景下,消费者想要实行删除权会更加困难[3],现有的法律条款也

未能有效促进权利的实现。

3.2. 电子商务个人信息保护缺乏有效监管

为了确保法律的有效施行, 政府部门需要承担宏观调控与整体协调的责任。当前, 监管体系的一个主要问题是机构职能的分散性。例如, 公安部门负责处理侵犯隐私权或频繁发送信息干扰公众日常生活的治安管理违法行为, 拥有行政监管权力¹; 国家网信部门则主要负责整体的协调与监督管理, 确保《个人信息保护法》得以有效实施²; 工业和信息化部及地方通信管理局则监督电信和互联网中的个人信息保护, 并在网络信息安全事件中协调处理³; 市场监管机构则承担市场监督和行政执法的职责⁴。

随着互联网、云计算、人工智能和区块链技术的飞速发展, 电子商务的专业性显著增强, 这也使得该领域的监管和审查变得更加复杂。在实际操作中, 部分执法人员在相关技术领域的知识不足, 对个人信息的收集和应用的必要性与合理性理解不够深入。虽然政府部门会依法查处侵犯消费者隐私的行为, 但执法人员的专业知识与技能不足, 导致他们在保护消费者权益方面的能力有限, 这削弱了政府的执法效力。科技的持续进步意味着个人信息保护不仅需要依赖传统的数据收集与处理方法, 还需要高度的专业技能。尤其是在处理严重的信息滥用问题时, 这给政府在市场监管方面带来了越来越多的挑战。信息技术的发展与缺乏专业技术工具和技术人员之间的差距, 给个人信息保护带来了额外的考验[4]。

3.3. 电子商务个人信息保护缺乏充分救济

第一, 法律责任归责困难。在审理侵权案件中, 法庭要求消费者提出的证据必须直接指向被告——电商经营者, 并证明此行为与消费者受损的权益有直接的因果关系。由于网络购物涉及多方, 如电商平台、商家、支付和物流服务提供者, 甚至可能包括过程中的任何未知第三方, 这些都可能是侵权行为的实施者。因此, 要求消费者准确识别侵权主体是非常复杂的。加之网络环境下侵犯个人信息的手段较为隐秘, 大多数消费者在遭受侵权后很少采取主动维权, 成功的诉讼案例更是少见。

第二, 未引入惩罚性赔偿制度。在遭遇侵犯隐私的欺诈或盗窃事件时, 虽然消费者可能获得一定的经济赔偿, 这类赔偿通常只能补偿实际损失, 而无法达到惩罚效果。网络运营者从大型互联网公司到小型个体经营者众多, 对这些不同规模的运营者实施相同的处罚, 对大公司的威慑力明显不足。鉴于通过法律途径获得的赔偿往往与个人信息的潜在经济价值不成比例, 甚至需要消费者投入更多的时间和精力, 这降低了权利人通过诉讼维权的积极性。

根据《个人信息保护法》, 赔偿计算通常仅限于直接损失。在实际操作中, 确定实际损失本身就是一大挑战, 即便确定了损失, 法院也只会计算直接损失, 这种做法并未能真正补偿消费者的实际损失, 从而使得法律判决缺乏足够的威慑力。因此, 建立信息领域的惩罚性赔偿机制变得尤为重要。

4. 电子商务个人信息保护的纾解路径

4.1. 提升电子商务个人信息保护立法保护

4.1.1. 细化知情权保护条款

根据《个人信息保护法》, 在处理其个人信息时的知情程度必须是完全的, 并且其知情的方式应当

¹ 《治安管理处罚法》第 1 条: 为维护社会治安秩序, 保障公共安全, 保护公民、法人和其他组织的合法权益, 规范和保障公安机关及其人民警察依法履行治安管理职责, 制定本法。

² 《个人信息保护法》第 60 条: 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定, 在各自职责范围内负责个人信息保护和监督管理工作。

³ 《电信和互联网用户个人信息保护规定》第 2 条: 在中华人民共和国境内提供电信服务和互联网信息服务过程中收集、使用用户个人信息的活动, 适用本规定。

⁴ 《消费者权益保护法》第 32 条: 各级人民政府工商行政管理部门和其他有关行政部门应当依照法律、法规的规定, 在各自的职责范围内, 采取措施, 保护消费者的合法权益。

是清晰的。但在电子商务的法规制定中，关于“充分知情”和“明确”这一准则仍未形成一致意见。观察个人信息保护法实施前后情况，可见大部分电商平台的隐私同意仍采用“阅读—停留—点击同意”的模式。这种方式，加之条款的冗长和专业性，实际上并未确保消费者完全理解所同意的内容。

因此，首先应简化消费者的阅读负担，并增强电商经营者的告知责任。通过精简隐私条款中的非核心内容，用清晰且易于理解的方式初步告知消费者关于其个人信息的收集与处理信息。这不仅符合《个人信息保护法》第四十八条关于个人有权解释信息处理规则的条款，也能提高处理的效率和时间成本。在此基础上，对消费者的同意声明，我们采用“明确表示同意”的方式。例如，设置一个空白区域，让消费者在阅读后手动填写“已阅读并充分理解相关隐私条款”，或使用简单的选择题形式。只要消费者能根据条款内容做出正确选择，即视为他们完全理解并同意了相关条款。

4.1.2. 细化删除权保护条款

对于电商平台的消费者而言，一旦他们的信息被搜集并传递，信息流涉及的参与方众多，逐一删除信息的任务变得异常艰巨。这主要因商家与物流服务提供者之间的紧密互动和信息共享机制所致。现行的《个人信息保护法》主要聚焦于个人与直接处理其信息的实体之间的关系，并明确规定个人有权要求信息处理者删除其信息。在电子商务领域，这种规定主要体现在消费者与商家的互动中；然而，该法律框架尚未充分考虑到电子商务环境中个人信息的易获取性和相关方复杂的互动关系。

电子商务环境中的复杂性使得消费者难以全面通知所有相关方，因此实现信息删除的权利变得更为困难。电商经营者因此承担着通知所有相关实体删除用户信息的责任。目前，电商平台在履行删除职责时，通常会将消费者的删除请求通知给第三方，并要求这些第三方也同步执行删除。这一过程目前仍是非强制性的，应当尽快将其转变为法定的强制性责任，并对未能有效执行该责任的平台施以惩罚。尤其是在《电子商务法》中，应进一步明确并详细规定信息经营者的责任，确保这些规定既具有法律约束力，又能在实践中有效操作。

4.2. 完善电子商务个人信息保护监管机制

4.2.1. 更新监管理念，贯彻预防性监管理念

《“十四五”电子商务发展规划》强调了采取包容和审慎的监管策略的重要性，旨在建立一个从始至终的全面监管框架，增强各部门之间的协调与合作。这种“包容审慎监管”理念是对应对网络市场新技术和业态的创新性回应，目的是在严格监管与促进产业经济发展之间找到一个均衡点。实施全链条监管，这不仅是一种关键的监管策略，也是一种思维方式，有助于加强电子商务领域的全面治理，从而提升监管的效果。

传统的事后监管方式在电子商务领域表现为反应迟缓，难以满足该行业的特殊性和快速发展的需求。在疫情推动的电商业态迅猛扩张的背景下，电商平台的市场地位相对于消费者而言越发显著。鉴于电子商务行业的这种发展趋势，需要将针对性的前期监管措施常态化，包括实施定期与临时检查、加强监管力度及提供业务指导等，全方位预防电商平台可能的消费者个人信息侵权行为。这种全方位的监管方法不仅能更有效地利用司法资源，还能为消费者个人信息权益提供更为多样化和灵活的保护方式。这种做法既满足了现代个人信息保护的法制化需求，也支持了电子商务行业的健康有序发展，实现了信息保护与信息利用之间的平衡。

4.2.2. 增设专职岗位，充分进行专门监管

《个人信息保护法》第六章对负责个人信息保护的部门进行了明确，维持了现有的监管框架。这一章节规定国家网络信息部门负责总体协调，而国务院的相关部门则根据各自职责进行个人信息的保护与

监管, 但并未建立专门或统一的监管实体。目前, 全球多国都将个人信息保护法律化视为关键步骤, 并已经建立了不同形式的监管机构。这些机构大致分为三类: 独立的监管机构、内嵌于其他组织的监管结构, 以及专门负责信息保护的职位。从 20 世纪 80 年代末到 21 世纪初, OECD 国家中的独立监管机构数量显著增长了三到六倍, 这突显了独立监管在整个监管过程中的重要性。

尽管借鉴国外的监管模式具有其优势, 但在实施时必须考虑到中国的实际情况。鉴于我国对个人信息保护的强烈需求, 建立一个类似于英国的“信息专员办公室”或日本的“个人信息保护委员会”的独立监管机构似乎是一个理想的选择。然而, 这种机构的建立既耗时又复杂, 可能无法迅速响应当前迫切的保护需求。因此, 考虑到现有的体制结构, 中国可以着手建立一个独立的个人信息监管机构。首先, 应当创建一个专门负责电商消费者个人信息保护的职位, 并对其实施特别监管。同时, 招聘具备丰富互联网背景和对现代“算法”技术有深入了解的技术专家作为执法人员, 特别针对新兴的“算法滥用”等侵权行为制定针对性的监管措施, 以更有效地保护电商消费者的个人信息。在建立了独立的个人信息监管机构之后, 将电商领域的信息保护官纳入此机构, 这不仅能统一监管体系, 还能满足当前的实际需求。

4.3. 健全电子商务个人信息保护救济方式

4.3.1. 降低消费者举证的证明力要求

在个人信息权益保护案件中, 消费者必须提供明确的证据, 证明他们遭受的损害与侵权行为存在直接因果关系, 并且这种侵权行为是导致损失的唯一原因。这一要求显示, 即使基于损害赔偿的原则, 消费者仍面临证明其他关键侵权条件的难题。因此, 笔者提出以下见解: 为使消费者在维权过程中经历更顺畅, 如果消费者能清楚描述涉及的交易的核心信息, 那么可以合理推断, 该经营者可能涉及非法使用信息的行为。具体来说, 首先, 在确定侵权行为时, 应采用“高度可能性”作为评判标准。例如, 如果消费者在某购物平台购物后, 收到一条详细描述订单核心信息的欺诈短信, 可以推断该交易中经营者很可能非法使用了信息。其次, 损害结果需要通过客观的危险性标准来证明。这里需要强调的是, 消费者的个人信息权遭侵犯不一定导致重大经济或心理损失, 但由于个人信息固有地关联财产和人格利益, 一旦经营者确实侵犯了信息权, 就可能使消费者的个人信息面临风险。最后, 证明损害结果时, 应将这种客观的潜在危险作为评估标准, 确保消费者能证实经营者的行为增加了损害发生的可能性。因此, 如果消费者提交的证据符合上述三个条件, 并且经营者未能提供充分反驳或证明其行为的证据, 那么经营者应承担相应的侵权责任。

4.3.2. 引入惩罚性赔偿制度

惩罚性赔偿, 亦称报复性赔偿, 是保护消费者权益的关键机制之一。当消费者无法准确证明其遭受的具体损失时, 此制度提供的赔偿额度较高, 有效补偿了消费者的经济损失, 并且能够有效阻止并威慑那些违背诚信原则的商家行为, 最大程度地减少消费者损失[5]。惩罚性赔偿的主要目的是通过对商家违法行为施加高额罚款, 以此达到惩罚和预防的双重目的, 从而确保市场的公平与经济的稳定运作[6]。

尽管我国《个人信息保护法》已经通过, 遗憾的是该法并未包括惩罚性赔偿的条款。鉴于侵犯消费者个人信息的行为相对容易发生, 如过度收集、未经授权公开及处理个人信息等, 实施惩罚性赔偿将更有效地起到法律的威慑作用。网络运营者通过收集大量消费者个人信息获得经济利益, 这增强了其市场竞争力, 导致过度收集和使用个人信息成为普遍现象。随着个人信息侵权事件的增多, 惩罚性赔偿成为一个切实需要的措施。目前, 我国对侵犯个人信息的行为处罚较轻, 而在电商平台上, 获取消费者个信息的成本低廉但收益颇丰。因此, 即便进行赔偿, 也通常仅限于消费者直接的损失, 这降低了消费者维权的积极性, 并增加了个人信息侵权的隐蔽性。消费者需要投入大量时间和金钱进行维权, 这在很大程度上削弱了他们对抗个人信息侵权的能力。综上所述, 实施惩罚性赔偿是必要的, 它不仅能为受害者提

供补偿，还能对侵权者施加有效的威慑。

5. 结语

在电子商务蓬勃发展的今天，特别是一些移动端应用，它们在为用户提供便利的同时，也频繁暴露出侵犯用户隐私的问题。这些 APP 在收集、储存和使用用户个人信息时，往往采用极其隐蔽的手法，导致广大消费者对电商平台产生了深深的不信任感。尤其是在这个信息爆炸、数据至上的时代，电商平台在保护用户个人信息方面所承担的责任愈发显得重要且紧迫。本文从电子商务个人信息保护的现实挑战出发，提出了提升电子商务个人信息立法保护、完善电子商务个人信息保护监管机制、健全电子商务个人信息保护救济方式等完善建议，使电商平台在个人信息保护方面形成更为完整的系统，为用户提供更加安全、可信赖的购物环境。

基金项目

2022 年江苏省研究生科研创新计划《乡村振兴背景下我国农用取水许可行政监管研究》(KYCX22_3579)。

参考文献

- [1] 高志宏. 隐私、个人信息、数据三元分治的法理逻辑与优化路径[J]. 法制与社会发展, 2022(2): 208-210.
- [2] 彭诚信. 论个人信息的双重法律属性[J]. 清华法学, 2021(6): 3-5.
- [3] 李晓安. 电子商务法中删除权的法经济学分析[J]. 北京行政学院学报, 2020(2): 89-96.
- [4] 高秦伟. 个人信息保护中的企业隐私政策及政府规制[J]. 法商研究, 2019(2): 16-27.
- [5] 杨立新. 《消费者权益保护法》规定惩罚性赔偿责任的成功与不足及完善措施[J]. 清华法学, 2010(3): 9-10.
- [6] 王利明. 惩罚性赔偿研究[J]. 中国社会科学, 2000(4): 114-115.