

电子商务中消费者个人信息保护研究

王玲

贵州大学哲学院, 贵州 贵阳

收稿日期: 2024年5月13日; 录用日期: 2024年6月3日; 发布日期: 2024年8月8日

摘要

在“互联网+”的背景下, 电子商务产业迅速发展。消费者的个人信息对其发展提供了重要助力。但是由于电商平台与商家对个人信息的利用, 使得用户的个人信息受到了严重的侵害。如何更好地保护消费者的个人信息, 促进电商行业长期健康发展, 是当前电商平台亟待解决的重要问题。本文在界定网络购物消费者的概念和特点的基础上, 结合司法实践, 阐释网络购物中消费者个人信息保护的独特性, 对信息泄露的成因进行深入剖析, 并在此基础上提出了与之相适应的对策。

关键词

电子商务, 消费者, 个人信息, 法律保护

Research on Consumer Personal Information Protection in E-Commerce

Ling Wang

School of Philosophy, Guizhou University, Guiyang Guizhou

Received: May 13th, 2024; accepted: Jun. 3rd, 2024; published: Aug. 8th, 2024

Abstract

Under the background of “Internet+”, the e-commerce industry has developed rapidly. Consumers' personal information has provided significant support for its development. However, due to the utilization of personal information by e-commerce platforms and merchants, users' personal information has been severely violated. How to better protect consumers' personal information and promote the long-term healthy development of the e-commerce industry is an important issue that e-commerce platforms urgently need to address. Based on defining the concept and characteristics of online shopping consumers, this article combines judicial practice to explain the uniqueness of protecting consumers' personal information in online shopping, conducts an in-depth analy-

sis of its causes, and proposes corresponding countermeasures accordingly.

Keywords

E-Commerce, Consumers, Personal Information, Legal 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

目前,随着电子信息科技的飞速发展,传统消费者的消费习惯已经发生了巨大变化,电子商务已经成为目前最为普遍的一种贸易模式,它已经渗入到了商品经济的各个方面,推动着商品流通和经济的融合。它突破了传统的物资交易方式,使物资的流动更加迅速和有序,使市场更加丰富和灵活。在网络交易中,用户的隐私保护已成为不可或缺的一环。在这样的背景下,如何更好地保护个人信息成为了一个亟待解决的问题。要想有效地保护好个人信息,除了要用科学的方式来保障公民的正当权益之外,还必须采取法律手段来预防和遏制个人信息的泄露。用户的个人信息是一种兼具人格与财产两种属性的数据,在大数据的累积过程中可以创造出财富价值,对促进电商交易与数字经济的发展有着重大的意义。

2. 电子商务中消费者个人信息保护概述

2.1. 电子商务的分类

随着数字化进程的不断加深,电子商务对人们的生活方式产生了深远的影响,促进了物资与信息的共享。在传统的交易中,由于个人信息的采集困难和使用效率低下,使得个人信息本身的产权属性难以体现。然而伴随着“互联网+”等新兴经济形式的涌现,线上消费呈现出繁荣景象,对个人信息的保护提出了新的要求。以交易主体为分类依据,可以将电子商务可分为以下四类:

第一种是 B2B (Business to Business)模式,以企业为交易主体。这种电子商务的交易方式已经发展了很多年,其中一个典型的例子就是商业公司通过电脑网络从供货商那里购买原料。

第二种是 B2C (Business to Consumer)模式,交易双方主体为企业和个人消费者。由于电商行业的兴起,这种类型的电子商务交易方式得到了迅速的发展,已经成为目前的一种主要的商务模式,就拿电商平台上的超市来说,提供的商品琳琅满目,应有尽有。

第三种是 C2C (Customer to Customer)模式,涉及电商平台的经营者和消费者之间的交易。商家在网络平台上报价,和消费者通过这个平台来进行交流,达成交易。这种交易方式是一种伴随着因特网的流行而快速发展的一种商业模式,适用于二手物品和收藏品的买卖。

第四种是“B2G”(Business to Government)模式,政企间的交易。在这种情况下,政府以消费者的身份和监管者的身份出现。例如政府在线上发布采购的详细信息,并通过竞价的方式招标。

2.2. 消费者个人信息的界定及保护的的特殊性

2.2.1. 对消费者概念与个人信息概念的界定

《消费者权益保护法》对消费者的概念进行了界定¹。法人和其他经济主体不是消费者,它们仅仅是

¹《消费者权益保护法》第2条:消费者为生活消费需要购买、使用商品或者接受服务,其权益受本法保护。

为了获得利润而采取的一种行动，并且在法律的价值和保护方法上，法人和其他组织以及个人消费者都存在着很大的不同。当前，世界各国对此采取了区分保护的方式，即对企业或其他组织采取了相关的反垄断法或商业秘密保护措施，以保障其经营活动中涉及到的数字与隐私的安全[1]。因此，本文将网络消费者定义为通过在线交易获得商品或服务，并支付了合理费用的个人。

对个人信息概念的界定。在《中华人民共和国个人信息保护法》第四条明确个人信息权利主体是个人²。消费者作为一般主体中的特殊部分，在购买、使用或接受服务的过程中，所提供或产生的能够标识特定身份的信息。这个问题的关键在于它是否能够被辨认出来，也就是说，它是否能够被识别为特定的顾客[2]。然而，由于消费者在交易的过程中，往往会提供或生成某些个人数据，这就需要对其加以拓展。随着科技的进步，电商经营者能够撷取到许多消费者并不能直接察觉但却具有重要价值的资讯。但是，如果仅仅以此为依据来认定消费者，则会造成认识上的局限性和范围上的不全面。为此，应对个人信息的保护范围进行扩展，并对“可识别性”的限度进行适度的突破。

2.2.2. 电子商务领域消费者个人信息保护的的特殊性

当前，我国针对消费者个人信息保护的法律法规已经越来越健全，但在互联网环境下，消费者的个人信息侵权事件还在不断发生，给消费者带来了极大的不安感。在网络环境下，消费者的个人信息保护具有以下特点：

一是具有很高的可辨识性。随着网络技术的飞速发展，利用大数据、智能技术等手段可以对用户的个人资料及具体消费行为进行快速、准确的识别。由于用户的个人信息具有很高的可辨识性，这给用户获得快速便捷的商品或服务的同时，对其个人信息的保护提出了严峻的挑战。为了精确地了解顾客的购买力和偏好，电商经营者利用大数据来分析顾客的消费偏好，从而获得更多的收益[3]。浏览器还可以根据用户的浏览偏好准确地投放广告来获得收入。

二是容易被入侵。互联网信息化和数据化的特点使得个人资料的获取、使用和交易已经形成了一条完整的产业链，泄漏的范围更广，危害性也更大。在电子商务中，用户的个人信息以“数据”的形式存在，为了避免下一次需要再次录入，“数据”一经上传，就会由网络运营商进行存储。对于一个人来说，当他将自己的信息提交上去之后，这个“信息”就已经不能称之为“个人”，而是成为一个可以供他人使用的“资料库”。随着大数据的快速发展，用户对自身信息的控制力逐渐减弱，相应的信息处理人员也逐渐将其掌握，从而对用户隐私保护的安全构成了极大的威胁。

三是具有很高的商业价值。随着电商产业的蓬勃发展，个人信息已经成为“数据资产”中最有价值的一种，一些人甚至无视《个人信息保护法》的规定，在追求高利润的同时，对用户生命和财产造成了极大的伤害。

3. 电子商务消费者个人信息保护存在的困境

3.1. 告知同意规则存在不足

告知标准简略。告知-同意条款是对个人信息保护的一项重要内容，这一条款是为了解决电商经营者和消费者之间存在着信息不对称的情况，处理者在对个人信息进行采集处理前，必须取得信息所有者的同意，并将其使用的用途和目的告知，从而保护其合法权益[4]。但是，现行法律条文对“充分性”缺乏明确的规定，造成了各种应用程序采集个人信息的标准不尽一致。在司法实践中，因为对个人信息保护政策的片面认知，法官也不能对消费者的真实目的作出正确的判断。特别要指出的是，在电子商务的背景下，很多企业或运营商都会用一种比较笼统的方式来表述“我们会与关联方和合作伙伴进行信息交

²《中华人民共和国个人信息保护法》第四条：个人信息是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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

换，以实现我们的业务目标”。由于缺乏有效的监督，消费者并不知道自己的隐私是如何被传递给各个企业，这就增加了消费者隐私泄露的风险。

3.2. 使用大数据算法进行杀熟

用户个人信息已成为企业竞争力的重要组成部分，而大数据平台上的数据分析与处理则是其典型的侵权行为。“大数据杀熟”是指将个体数据作为载体，借助大数据算法，在平台与用户间形成信息差。它最大的特征是灵活多变和极高的隐蔽性，使用者难以将已绑定信息全部解除。电商企业可以通过对消费者偏好、浏览记录等不敏感的信息进行深度挖掘，进而获得顾客的购物地点、种类、价格、停留时间等相关信息，并据此实施个性化服务、价格歧视或针对性广告投放，达到高效利用大数据的目的。

“大数据杀熟”的实质是针对相同的产品或服务进行差别化定价，进而对不同的消费者定价。电商平台持续采集、整理海量的用户数据，通过多年来的累积，并将其与其它平台进行整合，从而构成了“数据仓库”。运营商在搜集了海量的用户数据后，根据利益最大化的原则，为用户提供全面、个性化的营销服务，其中包括对原有用户的准确推送和差别定价，对新用户和价格敏感群体实行优惠的定价等。当消费者接受了电商平台的杀熟方式后，基于对电商平台的信赖和依赖，他们对价格的敏感度会降低，电商平台会再次进行新一轮的杀熟，从而获得巨大的经济效益。然而，现实生活中，个体难以对大数据杀熟行为进行有效取证，难以对其进行定性判断。因为电商平台通过大数据分析，为消费者提供了商品类别、品牌和价格等信息，无法实现“明码标价”，也无法满足消费者对商品价格的需求，并且价格也在不断变化。这样的“歧视”只能通过多方的比较来揭示。在现实生活中，当消费者对平台上商家的“大数据杀熟”进行投诉时，多数平台商家会依据季节、数量、地域、捆绑价格、动态价格等来说明“价格歧视”的正当性，由于缺少有效的证据，监管机构很难判定被投诉企业是否采用“价格歧视”，给消费者造成损失。

3.3. 司法救济不充分

3.3.1. 难以证明实际损失

消费者在遭到侵害后要求经营者承担损害赔偿、精神损害赔偿等民事责任。对于财产的损失，消费者很难准确地估算其所受的损失，也没有一个统一的衡量标准。在极个别的案例中，消费者确实遭受了财产上的侵害，而所能得到的补偿却只是经营者所得的极小部分，因而不能对经营者进行有效的警告和惩罚。就精神损害而言，必须符合“严重”的等级时，方可得到补偿，因而在很少的案例中，可得到补偿。例如“凌某某诉北京微播视界科技有限公司隐私权、个人信息权益络侵权责任纠纷案”³。“赵鹏与杨喜东等隐私权纠纷案”⁴中，法官认可了原告因为个人信息权利所受到的经济损失，赔偿金额分别为1000元和10万元，但对原告提出的精神损害赔偿请求，法院均以被告未拿出对其造成严重精神损害的证据为理由，不予支持。

3.3.2. 法律责任归责困难

在民事侵权案件中，法院对消费者的举证提出了明确的要求，即侵权行为是由被告的电商企业实施的，并且与消费者利益受到的损害之间存在着因果关系。消费者个人信息权的侵权主体是不唯一的，网络购物平台、平台商家、支付服务提供者、物流服务提供者这几类主体都有可能是侵权者，甚至在信息流通的过程中，一个不知名的第三方也会变成侵权者，就难以确定侵权主体。在网络环境中，对其个人信息权益的侵犯手段往往是隐蔽的，这就使得许多消费者在遭受侵权的时候，难以积极地去维护自己的

³ 参见北京互联网法院(2019)京0491民初6694号民事判决书。

⁴ 参见北京市朝阳区人民法院(2018)京0105民初9840号民事判决书。

权益,更不用说胜诉了。在司法实践中,也有对归责标准进行改革的个案,在“申瑾案”⁵和“付全贵案”⁶中,法院对消费者证据证明力的要求从“单一方向”调整为“高度可能性”,但只有极少数案例采用这种方法。这表明,虽然司法机构对其归责标准进行了变革,但是还不够完善,仍需根据其特点,对其归责原则作出相应的调整。

3.3.3. 未引入惩罚性赔偿制度

在某些涉及个人信息的欺诈、盗窃等侵权行为中,由于消费者的财产遭受了明显的损害,因此可以得到一定程度的赔偿,但是这些损害赔偿只是一种补偿,而不能对其进行有效的惩罚进而达到警示作用。网络运营商的主体繁多,大到互联网大公司,小到个体户,对不同的主体都是一样的惩罚,对大公司已经没有了威慑力。在巨大的利益面前,个人信息所能获得的经济利益与通过法律途径获得的赔偿金额不相称,而且还会花费更多的时间和精力,这也导致了被侵权人没有通过诉讼来维护自己的权益。

3.4. 消费者个人信息保护的监督管理机制不健全

3.4.1. 政府监督管理机制不健全

为了确保法律的执行,政府部门应该起到宏观调控和统筹协调的角色,但是目前存在监督主体不够集中的情况。例如,公安机关对散布他人隐私或者多次发送他人信息干扰他人正常生活的治安管理违法行为行使行政监管职权⁷。工信部、各省市通信管理局负责对电信、互联网上的个人信息的保护工作进行监管,对发生在网上的信息安全事故进行协调处置⁸;负责市场监管工作的市场监管部门同时也是执法部门⁹。但是由于监督主体之间的责任划分不明确,导致了系统之间的相互制约,导致各个部门之间的监督很难形成合力。随着互联网、云计算、人工智能、区块链等技术的快速发展,电商行业越来越专业化,监管与监管的难度也越来越大。在实际操作中,许多执法人员由于对 cookie、哈希算法、NFT 等基本专业术语不了解,对其采集与使用的必要性和合理性认识不足,导致执法人员在执法过程中存在诸多问题。虽然政府部门会根据相关法律对侵犯消费者隐私的行为展开调查,但是在许多案件中,因为一些执法人员的专业知识、技术水平有限,无法有效地保障消费者的合法权利,这就导致了政府的执法力度不到位。随着科学技术的发展,个人信息的保护已经不仅仅是简单的数据收集、处理、使用等,它需要专业技能,尤其是在面临着信息滥用的时候,政府部门的监管工作面临着更多的困难,缺少更加专业的技术方法和技术人才,这给个人信息的保护发出了更大的挑战[5]。

3.4.2. 消费者个人信息权保障的行业自律缺失

在市场主体能够自行解决问题的前提下,政府不应该进行干预,也就是“监管辅助”的原则,而当市场的自我调节能力不能满足民众的需要时,政府就应该对其进行辅助。从辅助规制的角度出发,一方面要从法律上对用户的个人数据进行保护,另一方面要从行业自律的角度来强化对用户个人信息使用的监督。但是,当前行业自律对于消费者个人信息的保护还比较笼统,并未形成切实可行的、有效的保障措施,其主要表现为操作性差、缺少实践指导。同时,也存在着以保护用户隐私为幌子,进行违法交易的现象。由于当前的行业自律机制还不完善,不能充分利用自己特有的产业优势,要想保证市场秩序,就需要加大监管力度,严格实施有关市场准入标准,并制定一系列行之有效的激励和约束机制,以保证

⁵ 参见北京市朝阳区法院(2018)京 0105 民初 36658 号民事判决书。

⁶ 参见北京市第四中级人民法院(2019)京 04 民终 143 号民事判决书。

⁷ 《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。

⁸ 《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。

⁹ 《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。

企业和用户的权益[6]。在消费者个人信息保护工作中，电商经营者扮演着双重角色，既要根据个体需求高效地使用个人信息，又要根据经营者的身份对自己进行监督，并合理地使用个人信息。由于互联网平台是一个公众场所，违法信息的交易时有发生，所以，电商经营者应扮演好“守门人”的角色，严格监管有关经营者的行为。

4. 完善我国消费者个人信息保护的建议

4.1. 在信息收集阶段完善告知同意规则

在告知方法上，为使“充分性”的有关内容能更好的传递给消费者，电商企业应以清晰、易理解和便于查询的方式将有关的个人信息保护策略提供给用户。具体来说，就是在对用户的个人资料进行采集前，通过一个独立的窗口来完成对用户的个人信息保护条款的告知。在告知内容上，电商经营者应采用简单易懂的“用户友好型”的语言，将有关的信息处理过程告诉消费者，并用醒目的字体突出显示文字，供消费者查询。关于第三方分享信息，如果电商经营者基于商业实践的客观需求，对第三方和信息分享的范围进行界定，建立起一套有效的信息保障措施，严格按照《个人信息保护法》中的规定来进行，同时也要让消费者知道第三方以及信息分享的范围。

4.2. 提高大数据杀熟行为违法成本

首先，要在立法、司法和行政要在提高大数据杀熟行为违法成本上达成共识。增加违规成本，是为了实现消费者和运营商的利益均衡。目前，针对“大数据杀熟”行为的维权案例并不多见，只有通过加大惩罚力度，才能达到“消费者”和“经营者”的利益均衡。

其次，在立法、司法和行政层面上，要建立以提高违规行为成本的体制机制。相关法律法规尽快出台，针对不同类型的算法，对歧视行为和大数据杀熟行为进行专门的规定；在诉讼中，对处于弱势地位的消费者进行赔偿，从而增强他们的维权热情。

4.3. 完善我国网络消费者个人信息的司法救济

4.3.1. 统一法院裁判标准

相比于入驻运营平台和第三方物流平台的电商企业，线上消费者往往处于弱势。在互联网环境下，当用户的个人隐私被侵犯，在其财产遭受损害的时候，消费者难以与巨大的电商企业相抗衡，诉讼过程和诉讼费用对于消费者而言犹如一场“马拉松”，使其耗费了大量的时间与金钱成本。付出的成本与能够得到的赔偿往往不成正比，从某种意义上说，这就导致了消费者寻求司法救济的难度较大，并且其维权积极性不高。所以在确定赔偿金额时，必须由法律对相应的损失数额进行统一，这不仅包括了消费者自己被诈骗或窃取的金钱，还包括了住宿费、维权交通费、误工费用等。当出现个人信息侵权案件时，若能对其可能得到的补偿作出合理估计，则可增强其维权积极性。

4.3.2. 降低消费者举证的证明力要求

在进行个人信息权益维权的过程中，相关法律规定消费者必须举证证明其所遭受的伤害与侵权行为有因果关系，并符合“唯一指向”的标准，也就是造成损害的唯一原因。因此，为了让消费者的权益得到更好的保障，应该对违法行为的举证应以“极高的可能性”作为判断标准。如一名顾客在网上购买商品，收到了一条关于该订单的详细信息，那就说明这次交易的卖家很有可能是非法使用了对方的信息。对于损害结果的证明，只需以客观存在的状况作为认定的标准。只要消费者能举证表明，经营者的不当行为对自己的利益造成损害时，在经营者无法反驳或无法证明其过错的情况下，就可以确定经营者应当承担侵权责任，消费者就能得到赔偿。

4.3.3. 引入惩罚性赔偿制度

惩罚性赔偿,也被称为报复性赔偿,是一种保障消费者权益的重要制度,在消费者无法举证证明其实际损失的情况下,可以给予较高的赔偿,对消费者造成的经济损失进行有效补偿,对违反诚实信用的经营者也能起到很好的震慑作用,最大限度地弥补消费者的损失。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。惩罚性赔偿作为一种威慑手段,在一定程度上起到了威慑作用,可以有效地防止侵权行为的发生,维护市场公平,促进经济的健康发展。

4.4. 健全网络消费者个人信息保护的综合监督机制

明确各部门之间的责任,强化各部门之间的合作和分工。目前,我国对个人信息的保护还存在着权限重叠等问题,因此,有必要进一步厘清。其中包括:

第一,为了防止各监管部门之间出现职责不明、重复执法的情况,有必要对各个监管部门的职责划分与职权进行详细的规定,以防止由于执法不统一而导致执法公信力降低的负面效应,同时要健全协调机制,加强各个部门间的交流与合作,明确各自的职责,防止互相推诿,共同提高执法水平。

第二,要加强专业分工。在执法人员构成上,应配备法律、计算机、信息管理等专业人才,以确保执法队伍的专业化。对侵犯个人信息的情况有一定的了解,可以更专业地收集证据,为消费者提供更好的保护。同时,要建立健全的监督机制。例如,在预防和紧急情况下,在在侵权行为的早期阶段,就由被动的处理方式向内部控制型的监督机制转变,以防范于未然[7]。

5. 结论

在这个信息和数据飞速增长的年代,谁能够掌握更多的用户信息,谁就能站在时代的前列。然而,如果一个公司或一个产业仅仅是为了收集信息,而忽略了信息的保护,甚至会为了获取非法利润而故意泄漏用户的个人隐私,这对企业和产业的发展是非常不利的。这样的发展方式,不但会破坏社会的秩序,让用户失去对电商平台的信心,还会导致产业的混乱。为了适应时代的发展,满足消费者信息保护的紧迫需求,公司应该完善告知同意则,细化消费者个人信息的保护方式。政府部门要加大对大数据杀熟行为的处罚力度,健全消费者个人信息的监管和保障机制,法院应该在审判的时候统一裁判标准,降低消费者的举证标准,建立惩罚性赔偿制度。与此同时,消费者也要加强对个人信息的保护意识。总之消费者的个人信息保护需要各方的共同努力。

参考文献

- [1] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122+207-208.
- [2] 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, 28(2): 207-224.
- [3] 彭诚信. 论个人信息的双重法律属性[J]. 清华法学, 2021, 15(6): 78-97.
- [4] 程啸. 论个人信息处理者的告知义务[J]. 上海政法学院学报, 2021, 36(5): 67-80.
- [5] 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, 36(2): 16-27.
- [6] 刘权. 数据安全认证: 个人信息保护的第三方规制[J]. 法学评论, 2022, 40(1): 118-130.
- [7] 龙卫球. 数字化时代安全可信的法治保障与新型监管要求[J]. 传媒, 2021(18): 19-22.