

跨境电商中用户个人信息保护的困境与纾解

庞 静

浙江理工大学法学与人文学院, 浙江 杭州

收稿日期: 2025年5月26日; 录用日期: 2025年6月11日; 发布日期: 2025年7月9日

摘 要

作为外贸转型升级中的新兴形式, 跨境电子商务在我国对外贸易体系中的地位日益凸显, 已成为推动构建“制度型开放”新格局的重要支撑力量, 并在促进经济发展方面展现出强有力的作用。然而, 在涉及网络用户的个人信息保护方面却面临诸多困境: 一方面, 现行的个人信息保护标准相对滞后, 另一方面, 法律责任边界模糊、强制规范缺位以及整体安全保障机制尚不完善, 导致信息泄露现象频繁发生, 形势颇为严峻。为有效应对此类挑战, 应当在加强行政监管与平台自律并行的基础上, 推动国内法律体系的完善, 同时借鉴国际先进规则, 着力提升信息保护规范、明确法律责任框架、完善强制性制度安排, 并构建更加系统化、科学化的个人信息安全防护机制, 从而更好地保护用户个人信息, 为跨境电商行业的持续健康发展注入坚实力量。

关键词

跨境电商, 数据跨境, 个人信息保护

The Dilemma and Relief of the Protection of Users' Personal Information in Cross-Border E-Commerce

Jing Pang

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: May 26th, 2025; accepted: Jun. 11th, 2025; published: Jul. 9th, 2025

Abstract

As an emerging form of foreign trade transformation and upgrading, cross-border e-commerce is becoming more and more prominent in China's foreign trade system, and has become an important supportive force for the construction of a new pattern of "systematic openness", and has shown a

positive role in promoting the high-quality development of the economy. However, in actual operation, the protection of personal information of network users faces many difficulties: on the one hand, the existing standards for personal information protection are relatively lagging behind, and on the other hand, the blurred boundaries of legal responsibility, the absence of mandatory norms, and the imperfections in the overall security mechanism have led to frequent leakage of information, which is a rather serious situation. In order to effectively cope with such challenges, we should promote the improvement of the domestic legal system on the basis of strengthening administrative supervision and platform self-regulation, and at the same time, draw on international advanced rules, make efforts to improve the information protection standards, clarify the legal responsibility framework, improve the mandatory institutional arrangements, and build a more systematic and scientific personal information security protection mechanism, so as to effectively improve the safety and security level of the user's information and inject solidity into the sustained and healthy development of the cross-border e-commerce industry. This will effectively improve the level of security and protection of user information and inject solid impetus into the sustainable and healthy development of the cross-border e-commerce industry.

Keywords

Cross-Border E-Commerce, Cross-Border Data, Personal Information Protection

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. 跨境电商背景下个人信息保护的重要性

在跨境电商迅速发展的背景下, 个人信息安全保障的重要性愈发增强。伴随互联网技术的持续演进与全球市场一体化趋势的加深, 越来越多用户倾向于通过网络平台进行跨境购物与交易活动。然而, 信息泄露已逐渐演变为该领域不可回避的关键风险之一。从隐私权的基本保障角度来看, 确保个人信息不被滥用, 属于每位自然人应当享有的基本权利。在跨境交易过程中, 消费者往往需提交诸如姓名、联系方式、住址乃至银行账户等大量敏感信息, 一旦这些数据被非法使用或传播, 便可能对个体隐私权造成实质性侵害。进一步而言, 资金安全同样深受信息保护机制的影响[1]。跨境电商通常依赖在线支付完成交易流程, 消费者需要提交银行卡或信用卡等财务信息, 而上述数据一旦遭遇窃取, 极有可能引发财产损失及其他连带风险。

由此可见, 保障个人信息安全不仅是维护隐私权的前提条件, 更关乎交易中财物安全的基本保障。从平台提供个性化服务的角度出发, 跨境电商通常通过收集用户行为和偏好数据, 进行数据分析以实现精准推荐与定制化服务。这虽在一定程度上提升了用户体验, 但若缺乏足够的法律或技术手段对数据加以保护, 亦可能引发信息滥用, 进而对用户造成干扰甚至权益受损[2]。良好的信息保护机制是增强用户信任与确保平台可持续发展的重要支柱。在国际电商交易中, 商家与消费者之间的信任基础十分重要。一旦用户发现自身信息被泄露, 往往会削弱对平台的信任意愿, 甚至放弃后续交易行为; 而企业若无法妥善处理数据安全问题, 亦将在市场中失去信誉, 制约其长期稳定发展。因此, 建立健全的信息保护体系, 既是保障个人权益的制度需求, 也是推动跨境电商健康运行的内在动力。

2. 我国跨境电商个人信息保护立法现状

虽然目前我国跨境电商发展的势头迅猛, 但网络用户个人信息保护相关的法律规则仍然较少, 整体

制度设计尚未形成完善体系,表现为立法结构松散、规范内容不够细化。2021年8月20日,十三届全国人大常委会第三十次会议通过了我国首部以个人信息为核心保护对象的专门性法律——《中华人民共和国个人信息保护法》。该法为跨境电商场景下个人信息的使用和流通提供了基本制度框架与原则指引。其中第三十八条规定,若出于业务需求必须将个人信息传输至境外,信息处理者应采取有效措施,确保接收方的数据处理能力符合我国的法律要求。此条虽初步填补了个人信息跨境流动方面的法律空白,明确了处理者的义务,但内容较为笼统,缺乏可具体执行的操作细则,导致实效有限。配套规范方面,《电子商务法》第六十九条、第七十一条及第七十九条中亦提出电子商务经营者有义务保障用户信息安全,违反者将面临相应法律责任。两部法律在理念上协调呼应,形成合力以维护跨境交易中用户信息的合法权益。为了推动上述法律落地实施并增强其执行力,国家互联网信息办公室于2022年7月发布了《数据出境安全评估办法》(以下简称“评估办法”),对数据出境的具体标准作出系统规定。该“办法”通过其第三条、第五条及第八条,构建了我国首套数据出境安全评估机制,要求从数据传输目的、路径、类型以及境外接收方的合规能力等多个维度进行全面审查,旨在从技术和制度层面加强对跨境数据流动的安全控制。然而,目前相关立法与政策文件多集中于境内监管主体或电商平台经营者的义务安排,对网络用户本身的法律救济路径及其权益保护关注不足。例如,在用户信息遭泄漏或被非法使用时,如何救济、诉权边界何在、需取得何种形式的用户同意等关键问题仍未有清晰规定。此外,现行法律普遍采用以数据主体同意为前提的事前许可模式,《网络安全法》第42条即明确规定,网络运营方未经授权不得披露、篡改或销毁所收集的用户信息,也不得在未获用户许可的前提下向第三方提供信息。由此可以归纳出,我国目前主要以“数据主体同意+安全评估”相结合的事前防控机制为主导。然而,尽管此种做法可在一定程度上降低企业合规负担,并赋予个人更多自主选择权,但由于制度执行较为依赖个人行为意愿,客观上削弱了整体信息保护的强度,也在一定程度上暴露出我国在数据治理方面协调能力的短板。

从立法技术角度分析,当前制度在私法路径下的合规监管亦存在明显不足。目前的立法多从行政治理视角出发,缺乏对企业内部责任划分的具体规制,导致平台难以依托自身数据资源提供真正有效的“信息保护屏障”。例如,《公司法》《合伙企业法》《个人独资企业法》等均未将个人信息保护设为企业内部治理义务之一,企业在个人信息安全合规方面缺乏明确指引。对此,可借鉴《APEC 隐私框架》的做法,推动企业参与数据治理体系,探索以企业为支点的数据保护实践路径,从而推动建立多元参与、机制灵活的个人信息保障机制。

最后,从法律规范体系的整体构造来看,当前我国在跨境电商中对用户个人信息的保护规则呈现出条文分散、体系不统一的特点。相关规定不仅横向分布在多部法律之间,还纵向层级不一,缺乏体系性整合[3]。例如,《刑法修正案(七)》与《刑法修正案(九)》第二百五十三条对侵犯个人信息的犯罪行为作出了刑事定性,而《个人信息保护法》第六十六条则规定了相应的民事责任机制,两者分属刑法与民法体系,存在价值取向和适用标准不一的情况,增加了法律适用的不确定性,影响了用户权利实现的效率和成本。针对上述问题,有必要加快构建一个以宪法精神为统领、以基本法律为核心、由法律、行政法规与规范性文件共同构成的统一协调、分层递进的个人信息保护法律体系,为跨境电商中的网络用户提供稳定、明确、可救济的权利保障基础。

3. 跨境电商中用户个人信息保护的现实困境

3.1. 规则阙漏

受“公共利益优先”的法律政策取向影响,我国在长期的制度建设未能充分重视对个人信息的系统性保护。尽管近年来国家层面陆续出台了一些技术与管理方面的标准,试图弥补这一缺口,但遗憾的是,相关技术规范并非专门针对个人信息保护而设定,管理类标准亦多聚焦于计算机系统在传输过程中

对数据本身的安全保障,缺乏对信息权属主体的直接关注。2012年,中国出台了首个全国范围内针对个人数据保护的指导性标准——《信息安全公共及商用服务信息系统个人信息保护指南》,该指南由中国软件评测中心牵头联合多个机构共同制定,标志着我国在该领域的首次制度化尝试。此后,国家标准化管理委员会于2017年又发布了GB/T 35273-2017《信息安全技术 个人信息安全规范》,进一步细化了相关技术要求。在地方层面,也有部分城市进行探索,如大连市在2012年制定并发布了DB21/T 1522《软件及信息服务业个人信息保护规范》,西安软件园发展中心则早在2008年就公布了《陕西软件和信息服务业个人信息保护规范》。

从整体效果来看,当前我国现行的个人信息保护标准较为滞后,其内容多集中于数据收集与使用环节,对于信息公开、传输、共享以及泄露后的救济机制等问题涉及较少。这些规范基本上仍停留在上世纪60年代“公平信息实践”理念的框架之内,对目前个人信息保护的需求难以满足。企业在执行过程中也往往面临操作难度大、指引不足等问题,规范的实用性与适应性均有待提升。

随着大数据时代的到来,公众对于个人信息隐私的认知和重视程度显著上升,社会对构建严密信息保护机制的呼声日益增强。原有的信息安全标准已难以回应当下复杂多变的技术环境以及消费者对隐私权保障的实际需求。为了有效应对数字经济发展带来的新挑战,亟须推动制定更为精准、系统且具有高度适应性的个人信息保护标准,逐步形成一套既能体现本土法律传统,又能与国际惯例接轨的完整标准体系,从而在法治框架下构建起对公民个人信息权益的有力保护屏障。

3.2. 法律责任属性模糊

在跨境电商用户个人信息侵权相关的司法实践中,通常面临两种法律关系的交织问题:即究竟应适用侵权责任还是合同责任,用户应通过何种路径来维护自身合法权益。在当前的交易机制下,消费者若希望在跨境电商平台上完成交易,往往需先完成实名认证流程,而注册行为通常伴随签署包括《注册协议》《隐私保护政策》在内的相关文件。这些协议旨在明确用户与平台之间的权利义务结构,并规范平台对用户信息的收集、处理、使用与披露方式。依据合同内容,跨境电商平台负有保护用户个人信息安全的义务,若因平台管理疏忽、系统漏洞或故意泄露等原因导致用户数据被侵犯,消费者不仅可基于合同关系要求对方承担违约赔偿责任,还可能构成对用户人格权的侵害,触及信息安全权与知情权等核心权益。此类情形中,侵权与违约行为并存,从而形成法律上的竞合关系^[4]。

在“冯红真诉浙江天猫、淘宝中国侵权责任纠纷案¹”中,太原市中级人民法院在审理过程中未详细论证责任性质,而是直接援引《中华人民共和国消费者权益保护法》的相关条款,认定被告行为未侵害原告权益,最终驳回其请求。从审判方式看,该案以侵权为法律依据进行裁判,而在现实司法实践中,诸多基层法院(包括派出法庭)处理类似纠纷时,更多依赖合同违约的路径展开分析。

这种法律适用标准的不统一,在一定程度上暴露了我国法院在处理涉个人信息保护案件时存在“重实体、轻程序”的惯性问题。侵权责任与合同责任界限模糊,既可能影响法律关系的正确认定,也会削弱司法对权利救济的精确性与有效性。面向未来,需进一步明确二者适用条件与界定标准,厘清行为性质,科学选用法律依据,确保跨境电商用户在遭遇信息侵权时能够得到全面、及时的权利保障。

3.3. 强制性规则匮乏

自《个人信息保护法》(2021年)与《网络安全法》(2016年)陆续实施以来,跨境电商业务中涉及的个人数据流通逐步纳入法治监管的范畴。随着国家安全审查机制与数据本地化存储制度的确立,我国对于数据使用和保护所设定的法律门槛显著提高。然而,在实际运行中,上述制度在跨境电商背景下的

¹ 参见(2016)晋01民初1014号、(2017)晋01民终3531号裁判文书。

适用仍暴露出诸多制约与缺失。

一方面,国家互联网信息办公室在开展国家安全审查时,主要关注我国公民数据出境问题,采取的仍是一种单向审查机制。《网络安全法》未对外国数据流入我国境内是否需要经过相应审查作出规定,导致数据“入口端”的安全保障存在法律空白[5]。另一方面,为平衡产业发展与数据安全之间的张力,现行制度在适用范围上存在一定限缩,只是对重要信息基础设施的运营主体实施审查与本地存储义务,并未参照国际主流模式,将其适用范围扩展至所有网络参与方。此外,“个人信息”与“重要数据”的界定模糊不清,在司法实践中容易引发解释分歧,进而影响相关强制性规则的具体实施,增加了国际合作的不确定性与难度。

如果网络用户的数据遭到泄露并被境外不法组织滥用,势必将对国家安全构成实质威胁,甚至波及公共利益领域。在当前全球政治经济形势下,以中美贸易摩擦为代表的博弈格局持续升温,保护主义与“逆全球化”浪潮再度抬头[6],发达国家可能通过设定更为严苛的数据监管标准,试图限制我国在新型贸易领域中的发展空间。在此背景之下,跨境电商面临着空前的外部压力。我国亟须增强战略意识,从整体布局着手,构建覆盖范围广、制度环节完备、操作性强的数据强制性规则体系,以提升个人信息治理能力,在维护国家数据主权的同时,有效应对外部风险挑战,稳固跨境电商领域的法治根基[7]。

4. 跨境电商个人信息保护路径展望

4.1. 完善个人信息保护理念设计

在我国跨境电商用户个人信息保护的立法实践中,长期存在行政监管职责负担过重、而企业平台责任配置偏轻的结构性问题[8]。事实上,跨境电商平台在个人信息治理中不仅是被监管的对象,也应当成为规则落实的重要实施者和协同方。当前的制度构造,主要依赖行政机关履行数据保护监管职责,忽视了平台自主治理潜力的激发与利用,导致监管效能与现实需求之间存在错位。

回顾实践案例,企业平台在数据安全保障方面的角色不可或缺。2008年Facebook用户数据泄露事件,即反映出平台内部治理的失效,其信息被传送至剑桥分析公司并用于美国总统选举预测,引发全球舆论关注。最终,美国联邦贸易委员会(FTC)并未直接动用公权力,而是委托平台履行监管义务[9],表明行政监管与平台自治协同治理的重要性。因此,我国在构建跨境电商数据保护制度时,应确立行政监管与平台自我约束并重的治理理念。在数据跨境传输背景下,依靠行政机关单方面实施监督,存在力有未逮的现实难题;必须赋予平台更大的自治空间与法律责任,强化其内部治理体系。我们都知道企业天然具有经济利益驱动属性,在确保不侵害用户权益的前提下,应鼓励探索合理的数据使用机制,实现对数据资源的深度开发与合规利用。通过提高平台对数据价值的认知[10],推动其从被动合规向主动治理转型,实现企业治理能力与用户信息权益保护水平的双重提升。这种平台自治机制的升级,应成为未来个人信息保护制度的重要组成部分。

在制度建构上,还需立足中国实际,同时接轨国际经验。首先,应当对我国现行“知情同意”制度进行优化与细化。传统的同意规则作为法律授权的前提,在算法技术迅速发展的背景下面临实效性不足的问题,亟待修正。未来所有的数据收集和处理应继续以“同意”为核心前提,但应将同意形式进行类型化处理,包括明示同意、默示同意及有效同意等层级[11],并结合使用场景和潜在风险作出差异化响应。美国与欧盟提出的“场景风险平衡理论”便是此种制度发展的代表,其通过扩展信息主体的同意内容、加重数据处理者的义务,实现信息使用与数据保护的平衡。其次,应借鉴国际通行规则,构建符合中国国情的本土化个人信息保护体系。在国际层面,跨境电商数据保护机制以双边协议和多边协议为主,其中双边协议如2016年《欧美隐私盾》明确义务划分,监管可执行性强,而多边机制则在标准不一的背景下通过多边协调推动全球合作。我国可吸收这两种路径的有益经验,采用“保护为本、限制为辅”的制

度模型，即以维护数据自由流通与个人隐私为双重目标，在信息跨境流动与数据本地安全之间建立平衡机制。

未来制度设计应结合数据本身属性，实施差异化管理策略，结合数据主体授权、适当性评估机制及数据控制者保证制度^[12]，推动平台合规治理能力提升。在中国推动构建“人类命运共同体”的时代背景下，完善跨境电商个人信息保护法律体系，有助于提升我国在全球数据治理格局中的话语权，推动数字贸易高质量发展。

4.2. 完善个人信息保护配套机制

标准体系通常由具有专业资质的标准制定机构或行业组织设立，主要用于指导某一领域在技术、管理、操作、流程等方面的规范化发展。在个人信息保护领域，亦应遵循这一逻辑。根据标准化对象的不同，个人信息保护标准可细分为技术标准、管理标准、工作标准和服务标准。相较而言，技术标准与管理标准的规范性更强、适用性更广，故本文从这两个维度进行重点分析。

在技术标准方面，个人信息保护可细分为三项核心要素：信息共享、数据二次利用以及数据持有。其中，每一要素又可进一步拆解为若干属性。例如，二次利用可包括在相似情境下的再次使用、基于用户画像的定向使用，以及以市场营销为目的的再次使用等三类属性。从每个要素中选择一个属性进行排列组合，可组合出 36 种从宽松到严格不等的个人信息保护等级。这一模型的优点在于其细致入微的技术划分，允许用户在不同维度自主授权，从而实现对其个人信息的个性化保护。在管理标准层面，应当推广实施“个人信息影响评估”机制。当前，跨境电商平台中个人信息滥用与泄露事件频发，公众对信息安全的关注持续上升。个人信息影响评估制度可以在维护企业数据开发利益的同时，合理平衡消费者的数据安全需求。该制度不仅涵盖用户行为信息和人际沟通信息，还包括核心的个人数据信息，其评估流程包括信息交换、方案拟定、方案适配等环节，通过前置性评估机制，帮助平台预测潜在侵权风险并提供防范措施，从而构建起一道信息保护的“防火墙”。

跨境电商用户个人信息保护涉及侵权与合同两类法律责任，因而在适用法律规范时必须厘清其责任归属。传统法理上，侵权责任与违约责任的划分依据在于义务来源：若义务源自当事人之间的约定，则适用合同法体系；若义务来源于法律的普遍性规定，则归入侵权法领域。然而，随着合同制度的发展，合同履行中逐渐出现了大量默示义务与法定义务，特别是在涉及人身和财产安全时，当事人之间负有一定的合理注意义务，该义务往往兼具契约性与法定性，此时若违反该义务，既可能构成违约，也可同时构成侵权。

具体而言，跨境电商平台在处理用户个人信息过程中负有数据安全保护义务，这种义务既源自用户与平台之间的服务协议，也受到《民法典》《个人信息保护法》等法律的强制性约束。当用户个人信息遭受泄漏、滥用等情形时，该行为既构成对合同义务的违反，也侵害了用户作为自然人的人格权利。因此，仅依赖义务来源划分责任类型显得逻辑不完备、解释力不足。为此，可引入“利益载体”理论作为辅助分析工具。根据该理论，损害可区分为履行利益(expectation interest)和维持利益(reliance interest)。前者指当事人基于合同履行所预期获得的利益，通常与违约责任相对应；而后者则指权利人已有的、现状下的人身及财产权利益，对此类利益的损害构成侵权。在跨境电商平台违规处理个人数据时，用户的“维持利益”即其现有的个人信息安全受到破坏，因此将该类纠纷纳入侵权范畴更具理论合理性和现实适应性。

综上，在处理跨境电商中用户个人信息保护法律争议时，应当以义务来源为主要判断标准，辅之以利益载体理论，准确界定法律关系属性。就司法实务而言，更应鼓励将此类纠纷作为侵权案件审理，督促侵权方承担相应法律责任，从而更有效地保护网络用户的个人信息安全，推动我国数据治理体系的规

范化与法治化。

4.3. 增加强制性规则

实践表明,跨境电子商务已成为推动国家经济增长的重要引擎,并在全球经济体系中发挥着日益突出的价值。然而,当前跨境电商中个人信息保护领域存在“法不配位”现象,强制性法律规范的缺位导致传统法律规则难以在网络空间中有效适用,严重制约了我国在数字经济时代的信息治理能力。为完善制度体系、弥补法律空白,应从以下几个方面进行制度建构与完善:

首先,应修正和优化国家层面的数据审查制度。目前,我国由国家互联网信息办公室负责对个人信息跨境传输行为进行监管,并实行以数据“出境”为对象的单向性审查机制。然而,现实中对国家安全和公共利益构成重大威胁的往往是“入境”数据,即境外机构对我国网络空间的监控、情报搜集等行为。若对境外数据流入我国缺乏有效审查,势必将为不法分子和间谍组织的滥用行为留下漏洞,不仅威胁我国网络用户的个人信息安全,也有可能影响社会稳定,甚至损害国家安全。因此,构建双向审查机制,合理纳入境外数据流入的监管范畴,是弥补法律滞后、增强网络空间安全治理能力的重要举措。

应当完善我国的本地存储制度。所谓本地存储制度,是指要求网络用户在境内产生的数据必须存储于境内服务器中的强制性规则^[13]。目前,《网络安全法》第37条仅对“关键信息基础设施运营者”提出了本地存储的要求,其适用范围相对狭窄。相较之下,俄罗斯于2014年修订的《个人数据处理法》则对所有互联网上形成的个人数据实行强制本地存储。从我国跨境电商发展和战略自主性的整体考虑,全面采纳类似俄罗斯的模式尚不现实。一方面,严格限制数据跨境流动可能会对我国跨境贸易形成制度壁垒;另一方面,过度监管可能抑制数字经济创新。因此,在本地存储制度设计上,应坚持宽严有度的原则:不宜对所有个人信息实行强制本地化要求,而应通过适度扩大“关键信息”的认定范围,逐步增强数据监管能力,实现个人信息保护与贸易自由化之间的动态平衡。值得注意的是,《重要数据识别指南》尚未正式发布,未来在制度制定过程中可适当扩展“重要数据”的范畴,从而为完善本地存储制度提供制度支撑。

最后,应就“公共秩序保留”条款的引入问题持审慎态度。公共秩序保留虽与强制性规则有相似之处,但其适用范围更为宽泛,往往涉及一国的基本法律价值与社会道德底线。在实践中,一些国家(如德国)已将强制性规则与公共秩序保留并行适用,以应对更加复杂的法律冲突情形。然而,从我国目前的立法环境来看,公共秩序保留的广泛适用存在一定障碍。一方面,道德规范具有一定的不确定性和地域差异性,在我国这样地域辽阔、文化多元的国家中,难以形成统一的适用标准;另一方面,若对公共秩序保留赋予法院过大的自由裁量空间,容易导致司法适用的不确定性,与我国目前“法定主义”导向的立法趋势存在冲突。综上,在当前阶段引入公共秩序保留机制尚不具备成熟的制度条件,应保持审慎立场,待立法、司法与社会伦理进一步发展成熟后再行考虑。

5. 结语

跨境电商中网络用户个人信息保护复杂,涉及法律、政策和行业规范,且相关侵权纠纷与传统案件不同。目前尚无统一规则,传统保护措施难以适应,亟需完善。构建保护体系时,应结合现代法学理论修订传统规则,尊重企业自治,发挥行政机关、企业和个人协同治理作用,降低信息泄漏风险,平衡保护与产业发展,提供切实可行的中国方案。构建双向数据审查机制、本地存储制度优化以及审慎对待公共秩序保留制度为基本路径,逐步推动我国跨境数据流动与个人信息安全保护的制度协调与法治化建设,为数字经济时代的信息安全治理夯实法治基础。未来法律修订应借鉴欧盟《通用数据保护条例》和美国《消费者隐私权保护法案》经验,结合国情,吸收公共秩序保留和场景风险理论的精华,制定符合本土特色的保护制度。

参考文献

- [1] 朱晓娟. 论跨境电商中个人信息保护的制度构建与完善[J]. 法学杂志, 2021, 42(2): 87-96.
- [2] 董战山, 谭伟, 刘琳, 等. 跨境电商相关税收政策国际比较研究[J]. 国际税收, 2022(7): 58-67.
- [3] 徐瑞梓. 我国跨境电商中信息安全的法律保护[J]. 中国商论, 2021(3): 21-24.
- [4] 汪晶. 论合同和侵权冲突法的新发展——以亚洲为视角[J]. 贵州社会科学, 2013(10): 93-95.
- [5] 苏丽娜, 张乐. 美国外资国家安全审查机制的政治异化及其法律因应[J]. 国际贸易, 2022(3): 82-88+96.
- [6] 何力. 逆全球化下中美贸易战与国际经济法的走向[J]. 政法论丛, 2019(5): 3-14.
- [7] 吕尧. 个人信息泄露事件评析[J]. 网络安全和信息化, 2021(2): 29.
- [8] 孙琪. 我国跨境电商发展现状与前景分析[J]. 商业经济研究, 2020(1): 113-115.
- [9] 方兴东, 陈帅. Facebook-剑桥事件对网络治理和新媒体规则的影响与启示[J]. 社会科学辑刊, 2019(1): 102-109.
- [10] 孟涛. 基于“丰鸟数据之争”的数据财产的法律属性与保护路径[J]. 大连理工大学学报(社会科学版), 2019, 40(2): 77-84.
- [11] 衣俊霖. 论个人信息保护中知情同意的边界——以规则与原则的区分为切入点[J]. 东方法学, 2022(3): 55-71.
- [12] 赵骏, 向丽. 跨境电子商务建设视角下个人信息跨境流动的隐私权保护研究[J]. 浙江大学学报(人文社会科学版), 2019, 49(2): 58-71.
- [13] 赵海乐. 论我国数据本地化措施与 FTA 缔约的协调[J]. 国际经济法学刊, 2022(2): 29-40.