

电商平台个人信息保护立法完善

周翠彬, 代丽丽

武汉科技大学法学与经济学院, 湖北 武汉

收稿日期: 2025年9月7日; 录用日期: 2025年9月18日; 发布日期: 2025年10月21日

摘要

本文旨在分析我国电商平台个人信息保护的立法现状与不足, 探讨完善路径以平衡数字经济发展与用户权益保护。研究通过梳理现行法律法规, 对比欧盟GDPR严格保护模式和美国行业自律模式, 发现当前存在法律概念冲突、责任配置碎片化、跨境数据规则模糊等问题。结果表明, 需构建统一法律框架, 优化阶梯化责任体系, 细化跨境监管规则, 并引入行业自律与第三方认证机制。结论指出, 应通过法律修订、行业协同与国际协作, 建立科学高效的监管体系, 为数字经济健康发展提供法治保障。

关键词

个人信息保护, 电商平台, 立法完善, 跨境数据流动

Improvement of Personal Information Protection Legislation in E-Commerce Platforms

Cuibin Zhou, Lili Dai

School of Law and Economics, Wuhan University of Science and Technology, Wuhan Hubei

Received: September 7, 2025; accepted: September 18, 2025; published: October 21, 2025

Abstract

This paper aims to analyze the current legislative status and deficiencies in personal information protection on e-commerce platforms in China, and explore paths for improvement to balance the development of the digital economy with the protection of user rights. The study reviews existing laws and regulations, compares the strict protection model of the EU GDPR with the industry self-regulation model of the United States, and finds issues such as conflicts in legal concepts, fragmented allocation of responsibilities, and vague cross-border data rules. The results indicate that it is necessary to build a unified legal framework, optimize a tiered responsibility system, refine cross-border regulatory

rules, and introduce industry self-regulation and third-party certification mechanisms. The conclusion points out that through legal amendments, industry collaboration, and international cooperation, a scientific and efficient regulatory system should be established to provide legal guarantees for the healthy development of the digital economy.

Keywords

Personal Information Protection, E-Commerce Platforms, Legislative Improvement, Cross-Border Data Flow

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

个人信息保护是通过赋予信息主体权利、设定信息处理者义务以及建立监管机制,对个人信息的收集、存储、使用、传输等处理活动进行规范的法律制度体系[1]。近年来,我国已初步构建以《个人信息保护法》为核心,《电子商务法》《网络安全法》等为支撑的法律体系,为电商领域的个人信息保护提供了基本框架。然而,实践中仍存在法律规范协调性不足、责任配置失衡、新型业态规制空白等问题,导致个人信息泄露、滥用等现象频发。当前学术界对电商平台个人信息保护的研究多集中于立法现状描述与域外经验借鉴,缺乏对制度内在逻辑与理论基础的深入剖析。多数研究仍停留在“问题-对策”层面,未能充分融入规制理论、治理理论等跨学科视角,导致政策建议缺乏系统性与可操作性[2]。本文从立法协调性、责任配置科学性、跨境监管有效性等维度,系统分析现行制度的结构性缺陷,并提出兼具理论支撑与实践可行的完善路径。本文的独特贡献在于:第一,突破传统对策研究的局限,将个人信息保护问题置于数字经济治理的大背景下,融合法学与经济学理论,提升研究的学理厚度;第二,提出可操作的阶梯化责任模型与跨境数据分类监管机制,为立法与执法提供具体参考;第三,通过典型案例的深度剖析,揭示司法实践中法律适用的现实困境,增强论证的实证基础。

2. 我国电商平台个人信息保护的相关法律制度

我国已建立起层级分明、内容详尽的个人信息保护法律体系,涵盖法律、行政法规、部门规章及地方性法规。

2.1. 法律

在法律层面,电商平台个人信息保护主要受《个人信息保护法》《电子商务法》《网络安全法》《数据安全法》等专门性法律的调整,同时《刑法》《民法典》《消费者权益保护法》等一般性法律亦提供补充性规范。这些法律从基本原则、权利配置、义务设定及责任追究等角度,构建了电商平台个人信息保护的基本法律框架。

《个人信息保护法》作为核心法律,确立了合法正当必要、最小必要和公开透明原则,赋予用户知情权、决定权、查阅复制删除权等权利,并规定电商平台对敏感信息的单独同意义务、数据安全保护义务及高风险处理的事前评估义务,违规最高可处 5000 万元或上年度营业额 5% 的罚款¹。《电子商务法》

¹ 《中华人民共和国个人信息保护法》第 66 条第 2 款第 3 项。

重点规范电商平台处理个人信息的合法性, 强调知情同意, 禁止强制同意行为, 并对跨境数据传输作出专门规定。《网络安全法》要求电商平台履行网络安全保护义务, 如防止信息泄露和境内存储要求。《数据安全法》则细化数据分类分级管理和跨境传输安全评估。此外, 《刑法》规定了侵犯公民个人信息罪, 《民法典》明确个人信息权益的基本内容, 《消费者权益保护法》从消费者保护角度规范经营者行为, 共同构成电商平台个人信息保护的补充性法律依据。

2.2. 行政法规与部门规章

行政法规与部门规章层面对信息处理者作出了更为细致的要求, 在信息处理者义务方面作出了更为细致的规定, 并提出数据分类管理, 对于关键信息和更为私密的信息需要采取更加严格的措施来加强保护。

行政法规进一步细化信息处理者义务, 强化数据分类管理和关键信息保护。2011年修订的《计算机信息系统安全保护条例》要求电商平台采取技术和管理措施保障数据安全, 重要系统需完成安全等级保护备案。2021年《关键信息基础设施安全保护条例》对大型电商平台实施严格监管, 要求境内存储重要数据, 跨境传输须通过安全评估。2024年7月施行的《消费者权益保护法实施条例》禁止过度收集个人信息, 规定不得因用户拒绝提供非必要信息而拒绝服务, 并要求建立数据泄露应急机制。2025年1月施行的《网络数据安全条例》重点规范自动化决策, 禁止大数据杀熟, 要求算法透明公平, 并细化重要数据管理和跨境传输合规要求。

部门规章方面, 2013年工信部《电信和互联网用户个人信息保护规定》要求电商平台明示信息收集目的, 用户注销后需删除或匿名化信息, 违规可处1~3万元罚款²。2019年《儿童个人信息网络保护规定》对14岁以下儿童信息设置严格保护, 需监护人单独同意。2020年央行《金融消费者权益保护实施办法》规定支付类电商平台须单独明示金融信息使用规则, 不得超范围使用。同年修订的《侵害消费者权益行为处罚办法》将非法泄露个人信息列为欺诈行为, 最高处违法所得3倍以下罚款³。2021年《网络交易监督管理办法》要求电商平台显著公示信息处理规则, 禁止强制收集非必要信息, 违规最高可罚3万以下罚款⁴。2023年网信办《个人信息出境标准合同办法》规定跨境传输数据需签订标准合同并通过安全评估, 违者按照《个人信息保护法》等法律法规处理。2024年《促进和规范数据跨境流动规定》进一步细化数据出境规则, 完善监管框架。

2.3. 地方性法规与地方政府规章

地方性法规和地方政府规章主要围绕电子商务及数据领域的个人信息保护与数据合规管理展开, 呈现了在国家立法的框架下地方因地制宜细化规则的规律。

地方立法在国家框架下细化规则, 以发达地区为典型。2021年《广东省数字经济促进条例》要求电商平台建立数据分类分级制度, 禁止大数据杀熟。2022年《上海市数据条例》强调最小必要原则, 跨境数据传输需申报安全评估。《深圳经济特区数据条例》创新性禁止强制个性化推荐, 用户可一键关闭, 违规最高可处上年度营业额5%罚款⁵。《浙江省电子商务条例》要求公开个人信息处理规则, 不得强制收集非必要信息。

地方政府规章如2020年《浙江省公共数据开放与安全管理暂行办法》规定使用政府开放数据时需脱敏处理。2021年《北京市公共数据管理办法》要求企业依法保护用户隐私。《重庆市个人信息保护管理

² 《电信和互联网用户个人信息保护规定》第23条。

³ 《侵害消费者权益行为处罚办法》第15条。

⁴ 《网络交易监督管理办法》第41条。

⁵ 《深圳经济特区数据条例》第95条第1款。

办法》则要求电商平台设立个人信息保护负责人, 数据泄露需 24 小时内报告。

我国电商平台个人信息保护法律体系已形成多层次、全流程的监管框架, 从基本原则到具体操作规范, 从国家立法到地方细化, 逐步强化平台责任, 推动数据安全与用户权益保护。随着法规不断完善, 电商领域的数字治理水平有望持续提升。

3. 立法层面反思

随着数字经济的蓬勃发展, 电子商务平台已成为个人信息处理的重要场域。我国虽已初步构建起以《个人信息保护法》为核心, 《电子商务法》《网络安全法》为支撑的法律规范体系, 但在立法技术层面仍存在若干亟待完善的结构性缺陷。本章将从规范协调性、责任配置科学性以及制度覆盖全面性三个维度, 系统剖析现行立法体系的不足。

3.1. 法律体系不协调

在纵向法律位阶关系上, 我国电子商务领域的个人信息保护规范呈现出明显的层级紊乱特征^[3]。作为基本法律的《个人信息保护法》与作为特别法的《电子商务法》在核心概念界定上存在差异。前者采用个人信息与敏感个人信息的二元分类, 后者却引入私密信息这一独特概念。这种概念体系的不统一直接导致法律适用困境。2022 年杭州互联网法院审理的某电商平台数据纠纷案⁶中, 作为基本法的《个人信息保护法》与作为特别法的《电子商务法》存在概念体系冲突。前者采用敏感个人信息的二元分类, 后者则隐含私密信息概念。本案法院仅依据《个保法》认定涉案信息非敏感信息从而平台无责, 却未考量《电子商务法》可能对私密信息施加的更严格保护义务。这种法律适用上的选择性与回避, 正是两法概念不统一导致司法困境的体现, 暴露出纵向规范间的内在不协调。

在横向规范衔接方面, 部门规章与地方性法规的差异化规定加剧了体系混乱。商务部《网络零售平台合规管理指南》将设备识别码明确列为敏感个人信息, 而某些地方性数据条例却将其排除在保护范围之外。这种规范冲突使得跨区域经营的电商平台面临合规标准不统一的困境^[4]。更值得关注的是, 对新型数据形态如社交电商中的用户关系图谱、直播电商中的消费行为画像等, 各级规范尚未形成统一的认定标准, 给司法实践带来极大不确定性。

3.2. 责任配置存在冲突

现行法律体系在电商个人信息保护的责任设定上存在明显缺陷。一方面, 责任形式呈现碎片化。《个人信息保护法》以罚款为主要行政处罚手段, 而《电子商务法》第 83 条则规定了包括暂停业务、吊销许可证在内的多元处罚方式。这种制度设计上的不协调, 导致执法实践中容易出现尺度不一、处罚结果悬殊的问题, 同一违法行为在不同地区或依据不同法律可能面临轻重迥异的处理, 既违背过罚相当原则, 也损害了法律适用的统一性和权威性^[5]。

另一方面, 归责原则体系存在适用混乱。《民法典》第 1034 条对个人信息侵权适用过错责任原则, 而《消费者权益保护法实施条例》等规范却在特定消费情形中引入过错推定责任。这种立法层面的不一致, 导致司法实践中对电商平台是否尽到信息保护义务的判断标准难以统一, 相似事实的案件因归责原则适用不同而裁判结果差异显著, 最终削弱了司法的可预期性和公信力。

3.3. 新兴领域监管缺位

随着电子商务模式的不断创新, 现行立法在应对直播电商、社交电商、跨境电商等新兴业态时, 暴

⁶薛祥飞浙江淘宝网络有限公司隐私权纠纷案, 浙江省杭州互联网法院(2022)浙 0192 民初 4259 号民事判决书。

露出明显的滞后性与监管盲区[6]。在社交电商领域, 二级乃至多级分销模式导致个人信息在复杂代理网络中无序流转, 而现有法律对间接获取、共享个人信息的主体责任缺乏清晰界定, 造成监管与追责困难。直播电商中的数据合规问题更为突出, 包括主播与 MCN 机构之间数据共享的合规边界、大数据杀熟行为的认定标准、直播回放中个人肖像及行为数据的再利用权限等, 均缺乏具有针对性的规范指引, 导致执法依据不足、处罚比例显著偏低[7]。

跨境电商则面临数据跨境流动的规制难题, 尽管《个人信息保护法》原则上规定了出境规则, 但对实践中常见的境内收集、境外使用等场景缺乏操作细则, 既难以有效约束境内平台主体, 也无法与国际规则形成有效衔接, 导致监管实效不佳。总体而言, 新兴电商业态的快速演化已显著超出传统监管框架的覆盖范围, 亟待通过立法更新和规则细化予以响应。

4. 其他国家或地区的立法

在全球数字经济快速发展的背景下, 个人信息保护已成为各国立法关注的核心议题。欧盟与美国作为个人信息保护领域的代表性法域, 分别形成了严格立法与行业自律两种典型模式。我国电子商务领域的个人信息保护制度尚处于完善阶段, 通过比较分析这两种模式的制度设计、实施效果及内在逻辑, 可为我国立法提供有益借鉴。

4.1. 欧盟: 严格保护模式

欧盟的个人信息保护制度以《通用数据保护条例》(GDPR)为核心, 《通用数据保护条例》是全球隐私保护的标杆, 为其他国家的个人信息保护立法提供了宝贵借鉴[8]。同时, 它还被称为全球最严格的个人信息保护制度, 主要原因在于其广泛的适用范围、严苛的合规要求、高额处罚力度以及对个人权利的全面保障。

首先, 广泛的管辖权。GDPR 采用属地和属人双重标准, 不仅适用于欧盟境内企业, 还延伸至境外实体对欧盟居民数据的处理行为。例如, 2020 年 Facebook 爱尔兰案确认, 只要与欧盟市场存在实质联系, 即触发 GDPR 适用。这种无差别管辖推动了欧盟标准的国际化, 促使非欧盟企业主动合规。

接着, 严格的数据处理要求。GDPR 要求数据处理必须符合六项合法条件之一, 如用户同意或合同履行必要。同时, 企业需遵循隐私设计原则, 默认启用最高隐私保护级别, 并仅收集最小必要数据。高风险数据处理还需事先评估, 否则可能面临最高 2000 万欧元或全球营业额 4% 的罚款⁷。

再者, 全面的个人权利保障。GDPR 赋予用户被遗忘权、数据可携权和反对自动化决策权。被遗忘权允许用户要求删除不必要或非法处理的个人数据, 数据可携权支持用户跨平台迁移数据, 反对自动化决策权则确保用户免受算法歧视。这些权利覆盖数据全生命周期, 重塑了数字经济中的权力平衡。最后, 严厉的违规处罚。GDPR 采用阶梯化处罚机制, 一般违规最高罚 1000 万欧元或营业额的 2%⁸, 核心违规(如未经同意处理敏感信息)则翻倍[9]。责任主体涵盖数据控制者与处理者, 形成连带责任。我国在完善个人信息保护法律责任体系时, 可借鉴 GDPR 将经济处罚与企业规模相挂钩的做法, 同时细化连带责任的适用标准, 以构建更加科学合理的法律实施机制。

4.2. 美国: 行业自律主导模式

美国的个人信息保护制度相较于欧盟更为零散, 由联邦和州两级法律共同构成, 并通过分行业、分领域的法律和法规来保护特定类型的个人信息[10]。其中, 加州的《加州消费者隐私法》(CCPA)和《加州

⁷ 《欧盟通用数据保护条例》第 83 条, 属于较高一级罚款。

⁸ 《欧盟通用数据保护条例》第 83 条, 属于较低一级罚款。

隐私权法》(CPRA)更具代表性,以企业自律为显著特点。美国的行业自律主导模式由三个板块构成:企业自主承诺、行业协会主导、第三方认证。

其一,企业自主承诺。企业通过隐私政策、用户控制机制和透明度报告表明数据保护立场。例如,苹果要求 App Store 应用披露数据收集类型,微软定期发布执法请求报告。然而,隐私政策常被批评为冗长晦涩,实际保护依赖市场声誉和事后监管,如联邦贸易委员会对违规企业的处罚。

其二,行业协会。行业协会制定行业标准,提供认证与争议解决机制。成员企业需遵守行为准则,违规者可能面临公开通报、市场排斥等非法律处罚。这种模式填补了联邦立法空白,但执行力度依赖行业自律。

其三,作为行业自律模式的重要补充,美国个人信息保护体系中的第三方认证机制呈现出市场化与多元化的典型特征。专业机构和行业协会提供市场化认证,评估企业实际合规状况。认证结果通过商业合同产生约束力,如亚马逊要求合作伙伴通过 ISO 27001 认证。然而,认证标准差异较大,加州已通过《CPRA 实施条例》规范核心要求,避免企业认证套利。

我国在构建认证机制时,可借鉴美国市场化运作的经验,但需注意三点:建立认证机构准入的负面清单制度、制定全国统一的基准性认证标准、完善认证结果的法律效力认定规则。通过规范引导第三方认证的健康发展,可有效提升个人信息保护的整体水平。

5. 完善我国电商平台个人信息保护的建议

当前我国电商平台个人信息保护立法虽已初步形成体系,但仍存在规范协调性不足、责任配置失衡及新业态监管缺位等问题。借鉴欧盟严格保护模式与美国行业自律经验,结合本土实际,可从以下方面完善立法与监管机制^[11]。

5.1. 构建协调统一的法律框架

针对法律概念冲突与规范衔接不畅的问题,可参考欧盟 GDPR 的立法技术,推动核心概念的统一界定。建议由全国人大常委会出台立法解释,明确《个人信息保护法》中敏感个人信息与《电子商务法》私密信息的适用关系,消除司法实践中的认定分歧。同时,建立跨部门协调机制,由网信办牵头制定电商领域个人信息保护的统一实施细则,整合商务部、市场监管总局等部门规章中的差异化要求,特别是对设备识别码、用户画像等新型数据的认定标准予以明确^[12]。对于地方性法规,应设立备案审查制度,确保其与国家立法保持一致,避免跨区域经营的电商平台面临合规冲突。

在新型业态规制方面,需及时填补社交电商、直播电商等领域的立法空白。可借鉴欧盟对数据可携权和自动化决策的规制经验,要求社交电商平台建立二级分销网络中的数据流转记录制度,确保个人信息在代理层级间的传输可追溯。对于直播电商,应明确主播与 MCN 机构间的数据共享边界,强制平台公示直播回放中的肖像权使用规则,并将直播间大数据杀熟纳入《网络数据安全管理条例》的禁止范围。

5.2. 优化责任配置与归责原则

针对当前责任形式碎片化与归责原则不统一的问题,应构建阶梯化责任体系并统一适用过错推定原则。建议在《个人信息保护法》中引入以企业规模、数据类型、主观恶意及整改情况为核心考量因素的处罚模型。具体而言,可参考 GDPR 按营业额比例罚款的机制,对中小电商平台设定差异化处罚上限。对处理敏感信息、出于恶意或漠视态度、以及屡犯不改的情形设置更高处罚阶梯,实现过罚相当。同时,应整合《电子商务法》《消费者权益保护法实施条例》等规范中的处罚类型,构建“警告-罚款-暂停业务-吊销许可”的递进式责任体系,增强执法可操作性和统一性。

在归责原则方面, 电商平台个人信息侵权案件应统一适用过错推定责任。用户仅需证明损害事实与平台数据处理行为之间存在因果关系, 平台若不能证明自身无过错即应承担赔偿责任。此举可有效缓解用户举证困境, 并与现有消费者保护规范相衔接。此外, 可引入平台对商家数据活动的监督与连带责任机制[13]。若平台未履行对入驻商家数据处理行为的审核与监督义务, 需就商家信息侵权后果承担相应连带责任, 从而系统性强化电商生态中的个人信息保护责任约束。

5.3. 强化跨境数据流动监管

跨境电商的数据跨境规则亟待细化, 可结合 GDPR 的充分性保护原则与美国的白名单管理模式, 构建分类分级跨境传输机制[11]。首先, 由网信部门发布允许数据出境的目的地国家清单, 清单内国家需达到我国数据保护等效标准[14]。其次, 对金融、健康等敏感数据实施负面清单管理, 禁止向任何境外主体传输。最后, 对一般数据跨境, 要求电商平台签订标准合同并通过安全评估, 确保用户享有与境内同等的权利救济渠道。

为提升监管效能, 可借鉴美国第三方认证机制, 允许经备案的认证机构对电商平台跨境数据合规性开展评估, 通过认证的企业可简化安全评估流程。同时, 建立跨境数据流动的实时监测系统[15], 对违规传输行为实施动态拦截, 并探索与主要贸易伙伴的监管协作, 避免因规则冲突导致企业面临国际合规风险。

5.4. 引入行业自律与认证机制

美国行业自律模式对我国中小企业合规具有参考价值。建议鼓励电商行业协会制定行业数据保护准则, 如针对社交电商的《用户关系图谱使用规范》或直播电商的《消费者画像伦理指引》, 通过行业自律填补立法空白。同时, 推动头部平台公开透明度报告, 披露数据收集类型与使用场景, 增强用户信任。

第三方认证可作为法律监管的有效补充。由国家认监委牵头建立统一的个人信息保护认证标准, 涵盖数据收集、存储、跨境传输等核心环节, 并赋予认证结果法律效力。例如, 通过认证的电商平台在行政处罚中可获从轻处理, 或在民事诉讼中作为合规抗辩依据。为避免美国认证套利问题, 需对认证机构实施动态考核, 淘汰标准宽松的机构, 确保认证公信力。

5.5. 完善用户权利救济与协同治理

借鉴欧盟用户权利保障经验, 可在电商领域拓展被遗忘权的适用场景, 允许用户要求平台删除非必要留存数据, 如购物车历史或临时缓存信息。同时, 简化权利行使流程, 要求平台在 App 内设置一键行使权利功能, 集成访问、更正、删除等操作入口。

在维权渠道上, 可探索公益诉讼和在线仲裁并行的双轨机制。消费者协会可代表不特定用户提起公益诉讼, 解决个体维权成本高的问题。同时, 在电商平台内设仲裁机构, 由网信部门监督其独立性, 为用户提供快速纠纷解决途径。此外, 建立举报奖励制度, 对提供有效违规线索的用户给予现金或平台优惠券激励, 形成社会共治格局。

6. 结语

电子商务的快速发展在为经济增长注入活力的同时, 也对个人信息保护提出了更高要求。当前我国虽已建立以《个人信息保护法》为核心的保护框架, 但在电商领域的针对性、协调性方面仍存在提升空间。通过借鉴欧盟严格保护模式与美国行业自律经验, 建议从法律框架、责任配置与归责原则、跨境数据监管、行业自律和权利保障等方面完善制度设计, 以平衡技术创新与权益保障。展望未来, 需持续关注新兴业态的数据安全挑战, 加强国际协作, 通过完善立法、强化执法和提升公众意识, 构建符合国情且与国际接轨的个人信息保护机制, 为数字经济发展提供坚实保障。

参考文献

- [1] 程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学, 2019(4): 26-43.
- [2] 姚辉, 阙梓冰. 电商平台中的自治与法治——兼议平台治理中的司法态度[J]. 求是学刊, 2020, 47(4): 90-102, 2.
- [3] 李小草. 电商平台经营者角色演化及主体规范模式嬗变[J]. 现代法学, 2022, 44(5): 194-209.
- [4] 邹军, 胡小燕. 电商平台个人数据跨境流动的政策困境与治理进路[J]. 中国网络传播研究, 2018(2): 209-221.
- [5] 郭金良. 数字经济时代个人金融信息侵权保护的困境与应对[J]. 法学评论, 2024, 42(5): 120-130.
- [6] 周烁. 网络直播带货中直播平台的法律责任[J]. 法律适用, 2022(7): 133-144.
- [7] 徐明. 个人数字权利实现的立体均衡逻辑[J]. 法学评论, 2025, 43(4): 134-145.
- [8] 俞胜杰, 林燕萍. 《通用数据保护条例》域外效力的规制逻辑、实践反思与立法启示[J]. 重庆社会科学, 2020(6): 62-79.
- [9] 李昭熠. 欧盟个人数据保护立法对智能传播产业的冲击与启示[J]. 编辑学刊, 2019(4): 35-39.
- [10] 谢业华, 彭星, 张龙. 美国加利福尼亚州《消费者隐私法案》研究[J]. 征信, 2018, 36(10): 36-38.
- [11] 齐鹏. 中国与 DEPA 数据跨境流动: 规制差异及制度对接探究[J]. 法学评论, 2025, 43(3): 30-43.
- [12] 叶雄彪. 生成式人工智能背景下的个人信息保护: 范式转换与规则完善[J]. 法学家, 2025(4): 61-73, 192.
- [13] 张丽英, 史沐慧. 电商平台对用户隐私数据承担的法律責任界定——以合同说、信托说为视角[J]. 国际经济法学刊, 2019(4): 24-37.
- [14] 周莉欣. 电商平台自治法律机制的构建[J]. 法商研究, 2024, 41(2): 106-123.
- [15] 程莹. 元规制模式下的数据保护与算法规制——以欧盟《通用数据保护条例》为研究样本[J]. 法律科学(西北政法大学学报), 2019, 37(4): 48-55.