

大数据技术背景下个人信息法律保护的困境与完善

周紫萱

长春理工大学法学院, 吉林 长春

收稿日期: 2026年8月28日; 录用日期: 2026年9月17日; 发布日期: 2026年10月12日

摘要

随着大数据技术的广泛应用, 个人信息在收集、处理与流转中面临过度收集、算法黑箱与维权举证难等法律困境。尽管我国已出台《个人信息保护法》等法律法规, 但“告知-同意”原则形式化、自动化决策不透明、用户维权成本高等问题依然突出。本文从法理学与经济学双重视角特征切入, 分析当前个人信息保护面临的现实挑战与立法不足, 指出信息收集环节的强制授权、处理环节的算法歧视以及救济环节的举证困难是核心痛点。为此, 提出相应的完善路径: 重构“告知-同意”规则, 引入分层同意机制; 强化算法治理与平台问责, 保障用户拒绝自动化决策的权利; 优化司法救济, 实行举证责任缓和并推广个人信息保护公益诉讼。以期在促进数据要素合理利用的同时, 实现对个人信息的有效法律保护。

关键词

大数据, 个人信息保护, 告知同意, 算法治理, 法律规制

The Dilemmas and Improvements in the Legal Protection of Personal Information in the Context of Big Data Technology

Zixuan Zhou

School of Law, Changchun University of Science and Technology, Changchun Jilin

Received: August 28, 2026; accepted: September 17, 2026; published: October 12, 2026

Abstract

With the widespread adoption of big data technologies, personal information faces various legal

challenges during its collection, processing, and circulation—such as excessive data collection, the opacity of algorithmic systems, and the difficulty of providing evidence to safeguard users' rights. Although China has enacted laws and regulations—including the Personal Information Protection Law—significant issues remain, such as the formalization of the “informed consent” principle, the lack of transparency in automated decision-making, and the high cost for users to assert their rights. This paper adopts a dual perspective rooted in both jurisprudence and economics to analyze the current practical challenges and legislative gaps in personal information protection, identifying three core pain points: mandatory authorization during data collection, algorithmic discrimination during data processing, and the evidentiary burden in remedies mechanisms. To address these issues, the paper proposes corresponding improvement pathways: restructuring the “informed consent” rule by introducing a tiered consent mechanism; strengthening algorithmic governance and platform accountability to safeguard users' right to refuse automated decision-making; and optimizing judicial remedies by implementing a reduced burden-of-proof approach and promoting public interest litigation for personal information protection. These measures aim to facilitate the rational utilization of data as a production factor while ensuring effective legal protection of personal information.

Keywords

Big Data, Personal Information Protection, Informed Consent, Algorithmic Governance, Legal Regulation

Copyright © 2026 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

我们正身处一个由数据驱动的大数据时代。随着云计算、人工智能、物联网等数字技术的迅猛发展，数据的采集、存储、分析和应用能力呈指数级增长。个人信息作为数据资源的重要组成部分，其属性也发生了深刻变化：它不再仅仅是承载人格尊严与隐私利益的静态载体，更成为了具有巨大商业价值和经济潜力的“动态资产”。从精准营销、信用评估到智能推荐、用户画像，对海量个人信息的深度挖掘与聚合利用，在极大便利公众生活的同时，也成为了推动数字经济发展的核心引擎。然而，技术从来都是一把双刃剑。在大数据技术的加持下，个人信息的流转速度更快、处理过程更不透明、影响范围也更广，由此引发的法律风险日益凸显。实践中，移动应用程序(App)“一揽子授权”、“强制收集”非必要信息的现象屡禁不止；“大数据杀熟”、算法歧视等自动化决策问题层出不穷；而大规模数据泄露事件更是频发，给用户的财产与人格权益带来严重威胁。面对这些新型挑战，传统以“告知-同意”为核心的法律保护框架显得力不从心。面对冗长晦涩的隐私政策，用户往往只能被动点击“同意”，使得这一核心原则在实践中被严重“形式化”。同时，由于信息不对称和技术壁垒，个人在维权时常常面临举证困难、损害难以量化等现实困境。

从法理学的视角审视，上述困境的根源在于个人信息权益的权利属性模糊与保护模式的错位。尽管我国《中华人民共和国民法典》¹(后文简称《民法典》)与《中华人民共和国个人信息保护法》²(后文简称《个人信息保护法》)已明确将个人信息保护纳入人格权益范畴，但学界对于其究竟属于“隐私权”的延

¹<https://www.court.gov.cn/zixun/xiangqing/233181.html>

²http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html

伸,还是一项独立的“信息自决权”,乃至一种“个人信息权利束”,仍存在持续争议。这种权利属性的不确定性,直接影响了保护路径的选择。若将其视为绝对权,则“告知-同意”应作为铁律;但若承认其兼具社会属性与利用价值,则个人控制便不应是唯一模式。事实上,个人在面对强大的数据处理者时,既缺乏议价能力,也难以对信息的二次利用和聚合风险作出准确判断,这决定了单纯依赖个人意思自治无法实现对个人信息的有效保护,法律模式必须从“个人控制”向“合作治理”转型。从经济学看,隐私政策阅读成本、用户即时收益与远期风险不对称产生“隐私悖论”,信息不对称与负外部性使个人“知情-同意”在交易成本上不可持续^[1]。首先,信息不对称与高昂的交易成本使得理性用户无法真正“知情”。阅读并理解一份隐私政策所需的时间和认知成本,远超普通用户愿意支付的限度,导致“同意”沦为仪式性操作。其次,“隐私悖论”(Privacy Paradox)揭示了个体在面临即时便利与潜在风险时的非理性选择:用户理性上重视隐私,但行为上却为了微小的短期利益(如免费使用服务)而让渡权利,因为长期风险不可量化且概率未知。最后,个人信息具有公共物品属性与负外部性,一旦泄露,损害将由不特定的多数主体共同承担,而平台却无需承担全部社会成本。这种市场失灵决定了,仅靠个人意思自治无法达致隐私保护的帕累托最优,必须引入外部干预与制度重构。

在此背景下,如何平衡数据要素的高效利用与个人信息权益的切实保护,成为数字时代法学研究的重要课题。本文立足于我国《民法典》《个人信息保护法》等现行规范体系,结合大数据技术的运行逻辑,从法理学与经济学双重视角剖析“告知-同意”失灵的深层原因,并深入梳理当前个人信息在收集、处理与救济环节面临的法律困境。在此基础上,从重构同意规则、强化算法治理、优化司法救济等维度,提出完善我国个人信息法律保护制度的路径建议,以期为构建兼顾安全与发展的数字法治环境提供理论支撑与制度参考。

2. 大数据时代个人信息保护面临的法律困境

(一) 收集环节:过度收集与“形式化同意”

在个人信息全生命周期中,收集是数据流转的起点,也是当前法律风险最集中、用户感知最直接的环节。随着大数据技术的普及,各类移动互联网应用程序(App)往往以提供服务为由,通过“一揽子授权”、“不同意即不用”以及强制索取非必要权限等方式,对个人信息进行超范围收集。法理学上,若把个人信息视为个人可完全控制的绝对权,则“同意”应具全有或全无效力;但《个人信息保护法》第13条第1款第1项以“充分知情+自愿明确”为有效同意前提,第6条第1款要求目的明确合理、最小范围,说明立法已承认信息利用与人格保护并重^[2]。经济学上,冗长隐私政策使阅读成本高于单个用户预期收益,平台以“免费服务”置换广谱授权,用户理性选择“点击同意”,导致同意意愿与真实风险评价脱节。⁶近三年司法案例可验证该困境。最高人民法院指导性案例265号“罗某诉某科技有限公司隐私权、个人信息保护纠纷案”明确:某英语学习网站及应用程序在注册登录中收集职业、学习目的、学龄阶段、英语水平等用户画像信息,如不属于提供网络服务所必需且未设置用户拒绝提供后的替代登录路径³。该案将“合同所必需”与“最小必要”具体化,但对“非必需画像”的边界仍依赖个案目的审查,说明抽象同意规则在复合场景中存在适用成本。既有文献对“必需”提出行业清单化方案^[3],本文进一步认为应将法理上的权利束理论与经济学上的处理成本结合,用“功能-字段”映射替代概括授权^[4]。例如,许多工具类应用强制要求用户授权地理位置、通讯录或相机权限,否则拒绝提供基本服务;在注册账号时,用户被迫勾选包含数十项授权内容的“用户协议”与“隐私政策”,实质上丧失了自主选择的空间。这种乱象直接导致了我国《个人信息保护法》所确立的核心规则——“告知-同意”原则在实践中被严重架

³最高人民法院第47批指导性案例265号,罗某诉某科技有限公司隐私权、个人信息保护纠纷案,2025年8月28日发布;裁判要点见最高人民法院知识产权法庭:<https://ipc.court.gov.cn/zh-cn/news/view-4588.html>。

空。从法理上看,同意的前提是信息主体在充分知情的前提下作出自愿、明确的意思表示。然而,面对动辄数千字、充斥着法律术语且晦涩难懂的隐私政策,普通用户既无时间也无专业能力去仔细阅读和理解。为了获取便捷的数字服务,用户只能选择点击“同意”,这种“别无选择”的同意显然并非用户的真实意思表示[5],使得“告知-同意”机制沦为纯粹的“形式化”走过场。进一步而言,这种现象也折射出大数据背景下“隐私悖论”与“最小必要”原则适用的深层困境。一方面,用户理性上重视隐私,但行为上却为了便利不得不让渡权利;另一方面,大数据技术的核心价值在于对海量数据的聚合分析与二次挖掘,这使得信息的潜在价值在收集时往往难以准确预判。企业常以“提升用户体验”、“风险控制”或“个性化推荐”等模糊理由,不断扩大收集范围[6],导致法律难以对“最小必要”的边界作出清晰、可操作的界定。当同意变成形式、必要变成弹性,个人信息在源头上便失去了法律的有效保护,也为后续的数据滥用与泄露埋下了隐患。

(二) 处理环节: 算法黑箱与自动化决策风险

如果说过度收集是个人信息面临的第一道关卡,那么信息被收集后的自动化处理则让个人陷入了更为被动的“算法黑箱”之中。在大数据技术的驱动下,企业不再仅仅满足于静态地存储数据,而是通过复杂的算法模型对海量信息进行深度挖掘、关联分析,形成精细化的“用户画像”,并据此进行自动化决策。这种技术应用的普遍化,直接催生了“大数据杀熟”、精准推送导致“信息茧房”以及算法歧视等新型社会问题。例如,在消费领域,平台利用算法对同一商品或服务针对不同用户设定差异化价格,使得老客户反而面临更高的消费成本;在信贷、招聘等领域,基于历史数据的算法模型可能将某些群体的特征与“高风险”不当关联,造成隐蔽的歧视。这些现象的背后,是个人的消费习惯、行踪轨迹、社交关系等敏感信息被深度解析与不当利用。

然而,面对算法的自动化决策,个人往往处于“无知”与“无力”的状态,这构成了大数据时代个人信息保护的第二大法律困境——“算法黑箱”带来的不透明性与权利虚化。首先,算法决策的逻辑高度复杂且不对外公开,个人根本无法知晓自己的信息是如何被分析的,更无法理解算法是如何得出某个结论的。这使得《个人信息保护法》所强调的“知情同意”在处理环节彻底失效,因为个人连被处理的“逻辑”都无法知情,遑论“同意”。并且,尽管我国《个人信息保护法》第24条对自动化决策作出了规制,赋予了个人“拒绝权”并要求保障决策的透明度和结果公平,但在实践中这些条款缺乏具体的操作细则[7]。例如,当用户拒绝个性化推荐时,平台往往设置隐蔽的关闭路径,或是以降低服务质量为变相胁迫;而“算法解释权”更是面临技术门槛与商业秘密保护的双重冲突,个人难以要求平台以通俗易懂的方式解释复杂的算法逻辑。当技术壁垒与法律规则的模糊性叠加,个人在面对算法权力时便彻底丧失了制衡的能力,其合法权益在无形之中被侵蚀。

(三) 救济环节: 举证困难与维权成本高

在大数据时代,个人信息侵权呈现出隐蔽性强、技术性高、涉及面广的特点。当个人发现自己的信息被过度收集、滥用或泄露时,即便想通过法律途径寻求救济,往往也会陷入“维权无门”的窘境。这构成了当前个人信息保护面临的第三大法律困境——举证困难与维权成本高昂。

民事诉讼中“谁主张,谁举证”的一般原则,在个人信息侵权案件中让处于技术弱势的个人举步维艰。根据《中华人民共和国民事诉讼法》⁴的相关规定,原告需要证明侵权行为、损害后果、因果关系以及被告的过错。虽然《个人信息保护法》第69条规定处理个人信息侵害权益造成损害的,适用过错推定:处理者不能证明自己没有过错的,应当承担侵权责任。该条已缓解“谁主张谁举证”的弱势,但用户仍需证明“损害”与“处理行为对应关系”。经济学上,单条信息泄露边际损失小、聚合损失大,个人诉讼

⁴<https://flk.npc.gov.cn/detail?id=ff8081818a21dc13018b425303b7086d&title=%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E6%B0%91%E4%BA%8B%E8%AF%89%E8%AE%BC%E6%B3%95>

收益低于律师、取证、时间成本,产生集体行动困境。执法案例可补强该问题。最高人民检察院 2026 年发布个人信息保护检察公益诉讼典型案例:河北省保定市徐水区智慧停车场违规收集储存个人信息案,检察机关以行政公益诉讼检察建议督促多部门协同整改⁵;重庆市两江新区小区物业违法处理人脸信息案,针对人脸识别安全隐患督促网信与住建等履责⁶;浙江省杭州市临安区“网络开盒”侵害公民个人信息民事公益诉讼案,针对非法获取隐私信息主张公益损害赔偿⁷。上述案例说明:单个用户举证难的场景,可通过检察调查、技术鉴定与公益诉讼转化。既有民事救济研究强调过错推定与群体诉讼,本文进一步把“举证缓和”前置到隐私政策运行时审计,而非仅事后诉讼。

然而,在大数据场景下,数据的存储、传输和处理完全由平台掌控,个人既无法进入被告的后台系统查看日志,也难以证明平台存在安全漏洞或未采取加密措施。例如,在常见的数据泄露案件中,用户很难证明泄露源就是被告平台,还是自己在其他环节遭遇了钓鱼攻击。这种严重的信息不对称导致个人几乎不可能完成举证责任,最终往往因证据不足而败诉。其次,损害后果的难以量化进一步削弱了个人维权的动力。与传统侵权不同,个人信息侵权造成的损害往往是潜在的、无形的。一条手机号或身份证号的泄露,可能不会立即造成财产损失,但可能带来持续不断的垃圾短信、诈骗电话,甚至为未来的身份盗用埋下隐患。然而,法院在审理此类案件时,通常要求原告证明存在“实际损害”或“严重精神损害”,否则难以支持赔偿请求。这种严苛的损害认定标准,使得大量个人信息侵权案件因“损害微小”而不了了之。最后,维权成本与收益的严重失衡,导致个人缺乏提起诉讼的内在激励。面对大型互联网平台,个人不仅面临高昂的律师费、取证费和时间成本,还要承受漫长的诉讼周期。而即便胜诉,获得的赔偿往往也仅仅是赔礼道歉或象征性的经济赔偿,无法覆盖维权支出。虽然《个人信息保护法》第 70 条引入了公益诉讼制度,为大规模侵权提供了集体救济渠道,但目前公益诉讼的适用范围仍主要集中于侵害众多个人权益的重大案件,对于大量分散的、小额的信息侵权,个人依然面临“维权即亏损”的尴尬局面。当法律救济渠道因举证和成本问题而变得遥不可及,个人信息保护的法律规则也就失去了最终的威慑力与执行力。

3. 我国个人信息法律保护的现状与不足

(一) 现行规范体系:从分散立法到专门保护

经过近十年的立法探索,我国已初步构建起以《民法典》为基础、以《个人信息保护法》为核心、以《中华人民共和国网络安全法》⁸(后文简称《网络安全法》)、《中华人民共和国数据安全法》⁹(后文简称《数据安全法》)为重要支撑的个人信息保护规范体系。

在民事基本法层面,《民法典》人格权编明确了个人信息权益的法律地位,区分了隐私权与个人信息保护的不同路径,为个人信息保护提供了基本的民事请求权基础。在专门立法层面,《个人信息保护法》于 2021 年正式施行,标志着我国个人信息保护进入了全新的阶段。该法系统规定了个人信息处理的合法性基础、告知同意规则、敏感个人信息保护、跨境提供规则以及个人的各项权利,并设置了严格的法律责任,被称为中国版的“GDPR”。此外,《网络安全法》和《数据安全法》分别从网络安全防护和数据安全管理的角度,为个人信息保护提供了配套的制度保障。与此同时,国家还出台了一系列国家标准(如《信息安全技术个人信息安全规范》¹⁰GB/T 35273-2020)和司法解释,进一步细化了合规要求。可以

⁵最高人民检察院:个人信息保护检察公益诉讼典型案例(2026),河北保定徐水智慧停车场案。

https://www.spp.gov.cn/spp/xwfbh/dxal/202601/t20260122_716668.shtml

⁶同脚注 5,最高检 2026 典型案例,重庆两江新区物业人脸信息案。

⁷同脚注 5,最高检 2026 典型案例,浙江杭州临安“网络开盒”民事公益诉讼案。

⁸https://www.cac.gov.cn/2025-12/29/c_1768735112911946.htm

⁹http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html

¹⁰<https://openstd.samr.gov.cn/bzgk/std/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E>

说,我国个人信息保护的“四梁八柱”已经搭建完毕。

(二) 存在的不足:规则落地与治理效能的短板

尽管规范体系日趋完善,但在大数据技术的冲击下,现行法律在落地执行与治理效能上仍显露出明显的不足,主要体现在以下三个方面:

第一,原则性规定多,落地细则不足。《个人信息保护法》虽然构建了完整的制度框架,但部分关键条款仍停留在原则层面,缺乏具体的操作指引。例如,法律要求处理敏感个人信息应当取得个人的“单独同意”,但在实践中,何种形式的“单独告知”才符合法律要求?弹窗、勾选框还是独立的同意页面?法律并未明确。又如,对于“最小必要”原则,虽然要求不得过度收集,但不同行业、不同应用场景下的“必要”边界模糊,企业拥有过大的自由裁量空间。再如,针对自动化决策的规制条款,由于缺乏算法备案、评估的具体细则,导致“拒绝权”和“解释权”在司法实践中难以落地。这种“粗线条”的立法模式,使得企业在合规时无所适从,监管部门在执法时也面临标准不一的困境。

第二,监管力量分散,跨部门协同不足。当前,我国个人信息保护呈现“多头监管”格局。国家网信部门统筹协调,工业和信息化部门主管 App 违规收集,公安部门打击侵犯公民个人信息犯罪,市场监管部门处理消费者投诉。这种分工虽然覆盖了不同领域,但也容易导致职责交叉、推诿扯皮或监管真空。例如,用户遭遇 App “大数据杀熟”时,究竟应向网信办、市场监管局还是消费者协会投诉?实践中往往缺乏清晰的指引。此外,地方层面的监管力量相对薄弱,基层执法人员的技术素养和执法能力参差不齐,导致部分法律规定在基层执行时打了折扣,难以形成全国统一的监管合力。

第三,治理模式滞后:重事后惩罚,轻事前预防。目前的个人信息保护治理模式,仍带有明显的“运动式执法”和“事后惩罚”特征。监管部门往往是在媒体曝光、用户投诉或发生重大数据泄露事件后,才启动约谈、通报、下架或罚款等程序。这种“亡羊补牢”式的监管虽然能起到一定的威慑作用,但无法从源头上遏制风险。相比之下,国际通行的“隐私设计”(Privacy by Design)理念,强调在产品或服务设计之初就将隐私保护嵌入其中,而非事后补救。然而,我国现行法律并未将“隐私设计”或“数据保护影响评估”作为强制性的前置义务,企业缺乏主动预防的内在动力。在大数据环境下,一旦数据被违规收集或泄露,损害往往已经不可逆,单纯的事后惩罚难以弥补个人的权益损失。

4. 完善大数据背景下个人信息保护的法治路径

(一) 立法层面:重构“告知-同意”规则,细化落地标准

要打破大数据时代“形式化同意”的僵局,必须对传统的“告知-同意”框架进行重构,并填补规则落地的细则空白。首先,应引入“分层同意”与“动态同意”机制。对于非必要的个性化推荐、第三方共享等行为,平台不得采用“一揽子授权”的方式,而应通过独立弹窗、强制阅读计时等方式,让用户对不同类型的信息处理活动作出分别、明确的授权;当用户撤回某项同意时,平台不得拒绝提供核心服务。其次,应推动隐私政策的“简明化”与“可视化”。法律可要求企业将冗长的隐私政策提炼为“核心要点摘要”,或采用图表、信息图等通俗易懂的形式向用户展示,确保用户在充分知情的前提下作出真实选择。最后,针对“最小必要”原则落地难的问题,立法机关和监管部门应尽快出台分行业、分场景的“必要个人信息范围清单”,为企业划定清晰的行为红线,压缩其自由裁量的空间,使法律原则真正转化为可操作的合规指引。

(二) 治理层面:强化算法问责,落实平台合规义务

面对“算法黑箱”带来的不透明风险,法律治理应从“事后惩罚”转向“事前预防与过程控制”并重。一方面,需细化自动化决策的规制条款。明确算法解释权的行使条件与边界,要求平台在用户拒绝个性化推荐时提供便捷、无隐藏的关闭路径,不得以降低服务质量相要挟;对于涉及信贷、招聘、医疗

等重大影响个人权益的自动化决策,应赋予用户要求人工复核和干预的权利,打破算法对决策权的垄断。另一方面,应全面落实“守门人”责任,强化大型平台的算法问责。法律可将国际通行的“隐私设计”(Privacy by Design)理念确立为企业的法定义务,要求其在产品设计之初就将数据最小化、去标识化等保护措施嵌入架构之中。同时,建立算法备案与评估制度,对高风险的数据处理活动强制进行“数据保护影响评估”(DPIA),从源头上遏制算法歧视与数据滥用。

(三) 救济层面: 优化司法救济与监管模式, 实现多元共治

针对维权举证难、监管分散的问题,需构建“司法救济 + 监管协同 + 技术赋能”的多元共治体系。在司法救济上,应实行“举证责任缓和”原则。在个人信息侵权诉讼中,当原告提供初步证据证明其信息被被告处理且存在泄露风险或实际损害后,应由被告自证清白,证明其已尽到安全保护义务且不存在过错,从而缓解个人的举证压力。同时,应进一步降低个人信息保护公益诉讼的门槛,鼓励检察机关、消协对侵害众多个人权益的行为提起公益诉讼,并探索引入惩罚性赔偿,让维权不再“得不偿失”。在监管模式上,应整合网信、工信、公安等部门的监管力量,建立常态化的跨部门协同执法机制,明确“大数据杀熟”、算法歧视等新型问题的管辖归属,消除监管真空。此外,可引入“监管科技”(RegTech),利用大数据监测、隐私计算等技术手段对 App 的数据收集行为进行实时审计,实现从“人海战术”向“技术赋能”的监管升级,真正筑牢个人信息保护的法律防线。

5. 结语

大数据时代的到来,既为社会发展注入了强劲动能,也对个人信息保护提出了前所未有的挑战。本文从收集、处理、救济三个环节切入,揭示了当前“告知-同意”原则形式化、算法黑箱不透明以及维权举证困难等核心法律困境,并指出我国现行规范体系在落地细则、监管协同和事前预防方面仍存在短板。针对这些问题,本文提出应从立法层面重构同意规则、治理层面强化算法问责、救济层面优化司法与监管模式三个维度协同发力,推动个人信息保护从“事后惩罚”向“全过程治理”转型。个人信息保护并非要阻碍技术进步,而是要在数据要素的高效利用与人格权益的充分保障之间寻求动态平衡。随着生成式人工智能、联邦学习等新技术的不断涌现,法律规制必将面临更多未知课题。唯有保持制度的开放性与适应性,持续回应技术变革带来的新型风险,才能真正构建起兼顾安全与发展的数字法治秩序,让每个人在享受大数据红利的同时,也能拥有不被侵扰的数字尊严。

参考文献

- [1] 高志宏. 大数据时代“知情-同意”机制的实践困境与制度优化[J]. 法学评论, 2023, 41(2): 117-126.
- [2] 程啸. 论个人信息处理中的个人同意[J]. 环球法律评论, 2021, 43(6): 40-55.
- [3] 吕炳斌. 个人信息保护的“同意”困境及其出路[J]. 法商研究, 2021, 38(2): 87-101.
- [4] 武腾. 最小必要原则在平台处理个人信息实践中的适用[J]. 法学研究, 2021, 43(6): 71-89.
- [5] 万方. 个人信息处理中的“同意”与“同意撤回”[J]. 中国法学, 2021(1): 167-188.
- [6] 程啸. 论个人信息处理者的告知义务[J]. 上海政法学院学报(法治论丛), 2021, 36(5): 67-80.
- [7] 丁晓东. 基于信任的自动化决策: 算法解释权的原理反思与制度重构[J]. 中国法学, 2022(1): 99-118.