文章类型：论文| 刊号（ISSN）：3082-8295(O) / 2630-4759(P)

数字经济中“知情-同意”机制的实效性考察与制度完善

刘灌著　章锦鹏　苏华阳
南京审计大学法学院
DOI:10.12238/ej.v8i6.2687

[摘　要] 数字经济背景下，“知情-同意”机制面临形式化合规与实质公平的深刻矛盾。研究发现,用户认知局限、平台权力失衡及数据跨境流动冲突,导致同意机制普遍失灵。基于总体国家安全观,本文提出分层治理路径：立法层面细化动态同意规则,监管层面建立数据信托制度,技术层面开发智能同意管理工具。研究创新性在于揭示国家安全与个人权益的协同逻辑,并提出中国特色的同意实施框架,为全球数字治理提供兼顾安全与发展的制度范式。
[关键词] 知情-同意机制；个人信息自决权；数据主权
中图分类号：TL822+.6　**文献标识码**：A

The effectiveness of "informed consent" mechanism in digital economy and the improvement of system

Guanzhu Liu　Jinpeng Zhang　Huayang Su
School of Law, Nanjing Audit University

[Abstract] In the context of the digital economy, the "informed-consent" mechanism faces a profound contradiction between formal compliance and substantive fairness. Research has found that user cognitive limitations, platform power imbalances, and conflicts in cross-border data flows lead to widespread failures in the consent mechanism. Based on a holistic national security perspective, this paper proposes a layered governance approach: refining dynamic consent rules at the legislative level, establishing data trust systems at the regulatory level, and developing intelligent consent management tools at the technical level. The innovation of this study lies in revealing the synergistic logic between national security and individual rights, and proposing a Chinese-characteristic framework for implementing consent, providing an institutional paradigm for global digital governance that balances security and development.
[Key words] informed consent mechanism; personal information self-determination right; data sovereignty

引言

随着数字经济的迅猛发展,数据已成为核心生产要素,但个人信息安全与数据开发利用之间的冲突日益凸显。作为个人信息保护基石的“知情-同意”机制在实践中面临严重失灵：用户往往被迫接受冗长晦涩的隐私条款,平台通过“全有或全无”模式变相剥夺选择权,而数据的二次利用和跨境流动进一步架空同意实效。在此背景下,总体国家安全观要求构建兼顾数据主权与公民权利保障的新型治理框架——既要防范数据滥用对个人权益的侵害,又要避免过度收集制约数字经济发展,还需应对跨境数据流动中的国家安全风险。如何重构“知情-同意”机制以实现多方价值平衡,成为当前立法与监管亟待解决的制度命题。

本研究具有重要的理论和实践意义。在理论层面,通过深入分析“知情-同意”机制的运行困境,有助于厘清个人信息自决权与数据自由流通之间的张力,为构建兼顾隐私保护与数据要素市场化配置的理论框架提供新思路。在实践层面,研究立足于我国《个人信息保护法》的实施现状,针对同意规则过于原则化、可操作性不足等问题,提出细化的制度完善建议,有助于健全配套机制,提升法律实施效果,既强化个人信息权益保障,又促进数字经济健康有序发展。

1 “知情-同意”机制的理论基础与法律定位

1.1法理溯源。“知情-同意”机制的法理基础源于个人信息自决权理论,该权利经历了从传统隐私权消极防御到现代数据控制权积极支配的范式转变。[1]在合同法视域下,有效的同意需符合意思表示真实性要求,包括信息充分披露、自由选择等要素,但数字经济中格式条款的普遍化使这一要求面临挑战。两大法系均通过判例(如德国“人口普查案”)或立法(如欧盟GDPR)确认：知情同意不仅是技术性程序,更是实现个人信息自主管理的核心法律工具。

文章类型：论文| 刊号（ISSN）：3082-8295(O) / 2630-4759(P)

1.2数字经济中的特殊挑战。数字技术放大了传统同意机制的局限性：一方面，数据聚合效应使单一同意延伸至不可预见的应用场景，导致用户陷入“同意疲劳”；另一方面，算法黑箱遮蔽数据处理逻辑，即使形式化披露信息，用户仍难以实质理解风险。平台通过界面设计（如黑暗模式）和复杂权限捆绑，进一步削弱同意的真实性与针对性，造成“同意即弃权”的实践悖论。

1.3总体国家安全观的制度约束。总体国家安全观将数据安全纳入国家安全体系，要求“知情-同意”机制在保障个人权益的同时，必须满足数据主权维护和关键基础设施保护等目标。《网络安全法》确立的数据本地化存储、《数据安全法》构建的分类分级保护制度，为同意机制划定了刚性边界。[2]当个人数据涉及国家安全时，同意自治需让位于公共利益，形成“个人控制-企业合规-国家监管”的三层治理架构。

2 “知情-同意”机制的实效性困境

2.1形式化同意普遍存在。当前“知情-同意”机制在实践中呈现出严重的形式化倾向，其有效性被多重因素削弱。[3]从用户端看，认知局限导致实质同意难以实现：隐私协议普遍存在篇幅冗长（平均字数超2500字）、专业术语堆砌等问题，配合“默认勾选”等设计，使用户在未充分理解的情况下被动授权。从平台端看，权力不对称性扭曲了同意本质：平台通过“全有或全无”（take-it-or-leave-it）模式迫使用户整体接受条款，重要数据收集行为被隐藏在次级菜单中，而“不同意即不可用”的设定更使选择权形同虚设。这种形式化运作使同意沦为合规幌子，未能真正保障用户自主权。

2.2动态数据处理中的同意失效。数据流动的动态性与同意机制的静态性之间存在根本矛盾。一方面，数据二次利用和第三方共享超出初始同意范围：用户往往不知晓其数据被转售给广告联盟或用于AI训练，而概括性授权条款成为平台规避责任的工具。另一方面，数据全生命周期管理缺位：同意撤回机制存在技术障碍（如区块链存证数据难以彻底删除），且缺乏对已聚合匿名化数据的处理规则。更突出的问题是，大数据分析产生的衍生数据是否仍需同意缺乏法律界定，导致“同意链条”在数据处理环节中断。

2.3跨境数据流动的特殊矛盾。全球化场景下的同意机制面临主权逻辑与个人自治的价值冲突。国际层面，GDPR充分性认定与我国《数据安全法》的本地化要求存在张力。[4]欧盟以个人数据权利保护水平作为跨境传输条件，而我国将重要数据出境安全评估列为强制性义务，个人同意在国家安全审查前效力受限。国内立法亦存在模糊地带：《个人信息保护法》第38条虽规定跨境传输需单独同意，但“非重要数据”的认定标准不明，企业常利用此漏洞规避监管。这种冲突揭示了数字经济时代同意机制的根本困境——个人意志如何在数据主权框架下获得实质性尊重。

3 域外制度比较与经验镜鉴

3.1欧盟GDPR的“严格同意”模式。欧盟《通用数据保护条例》（GDPR）构建了全球最严格的同意标准体系，其核心特征体现为两个层面：在同意形式上，要求采用分层同意（granular consent）设计，即对不同数据类型和处理目的分别获取明确授权，禁止捆绑式同意，并通过“动态同意”（dynamic consent）机制允许用户随时调整授权范围；在实施保障上，建立数据保护影响评估（DPIA）制度，强制企业在处理高风险数据前开展系统性风险评估，并由监管机构审查同意获取流程的合规性。这种模式虽有效提升了同意质量，但也面临实施成本过高（中小企业合规负担达年均€75,000）、用户选择疲劳加剧等问题。[5]值得注意的是，GDPR第49条为跨境数据传输设置的“明确同意”（explicit consent）特别要求，与我国《数据出境安全评估办法》形成鲜明对比，反映出不同法域对同意机制功能定位的根本差异。

3.2美国CCPA的“选择退出”模式。美国《加州消费者隐私法案》（CCPA）采用市场导向的“选择退出”（opt-out）机制，其制度逻辑体现三个特点：一是将同意场景限定于敏感数据处理（如生物识别信息）和未成年人数据收集，对一般商业数据实践则推定用户默示同意；二是通过“请勿出售我的个人信息”（Do Not Sell My Personal Information）的标准化退出通道，降低用户行权成本；三是建立“隐私权诉讼”（private right of action）制度激励企业合规。[6]这种模式虽提升了商业效率（企业数据流转成本降低约30%），但也存在重大缺陷：研究发现83%的用户从未使用退出权，且企业通过复杂跳转页面变相阻碍退出操作。[7]更本质的问题在于，CCPA将个人信息视为商品属性的立法取向，与我国《个人信息保护法》强调的人格尊严保护存在价值冲突。

3.3可借鉴要素与本土化适配。结合我国制度环境，可从域外经验提炼三项适配性改革路径：其一，建立差异化同意标准，对生物识别、医疗健康等敏感信息采用GDPR式“明确同意”，[8]对一般商业数据则可借鉴CCPA设置便捷退出机制，但需通过《个人信息分类分级指南》细化操作标准；其二，引入技术增强型同意工具，如基于区块链的同意存证系统（用户授权记录上链存证，实现全程可追溯），或开发标准化同意管理平台（统一管理各APP授权状态）；其三，构建“同意有效性评估”制度，要求企业定期审计同意流程是否符合“自由、知情、具体”要求，[9]并将评估结果纳入《个人信息保护认证》体系。这些改革需平衡安全与发展双重目标，在《数据二十条》框架下探索具有中国特色的同意实施范式。

4 总体国家安全观下的制度完善路径

4.1立法层面。我国应在《个人信息保护法》实施细则中构建更具操作性的同意规则体系：首先，通过《个人信息处理告知指南》明确“知情”的实质性标准，要求企业采用可视化协议（如信息分层折叠、图标标注风险等级）和场景化告知（根据使用场景分段披露），[10]并严格贯彻最小必要原则，禁止将非必要权限与基础服务捆绑；其次，引入“动态同意”（dynamic consent）制度框架，规定数据用途或共享范围发生实质性变更时需重新获取同意，并建立梯度式授权机制（如设置“仅本次使用”“三个月内有效”等选项）。特别需要针对大数据分析、AI训练等新型处理目的，在《数据要素流通若干规定》中设定特殊的同意获取规则，平衡技术创新与权利保障。[11]

4.2监管层面。监管改革应着力构建同意机制的全周期治理

体系：一方面，由网信办牵头制定《平台同意设计合规审计指引》，重点审查黑暗模式(dark patterns)使用情况，要求企业留存同意日志以备抽查，并将审计结果纳入企业信用评价；另一方面，试点数据信托制度，授权具备资质的第三方机构(如个人信息保护合规协会)代表用户统一管理授权事项，解决个体维权举证难问题。[12]可参照英国ICO的“数据保护影响评估”模板，要求处理超过百万用户数据的企业定期提交《同意有效性评估报告》，通过监管科技(RegTech)手段实现动态监测。

4.3技术层面。技术赋能是提升同意实效的关键突破口：国家应主导开发统一数字身份系统，集成跨平台授权管理功能，用户可通过“一账通”查看和撤回所有APP的授权；[13]同时制定《人工智能应用于知情告知的技术标准》，要求高风险处理场景部署智能说明系统(如通过NLP技术生成个性化风险摘要，利用知识图谱可视化数据流向)。[14]对于区块链存证、联邦学习等新技术应用，需在《个人信息保护认证实施规则》中明确技术合规要求，确保可撤回性与不可篡改性并存。

4.4国际协作层面。我国应通过多边机制提升同意规则的国际话语权：短期内，优先与东盟、RCEP成员国协商建立“白名单”式跨境同意互认机制，对通过我国个人信息保护认证的企业简化出境流程；[15]中长期则需主动参与DEPA、CPTPP等数字贸易协定谈判，推动将“差异化同意标准”纳入国际规则。建议在“一带一路”数字合作框架下设立跨境数据流动特别工作组，开发兼容GDPR与我国标准的同意管理工具包，为发展中国家提供技术援助。同时，依托《全球数据安全倡议》，倡导构建兼顾国家安全与个人权利的同意实施国际准则。

5 结论与展望

5.1研究结论。本研究系统揭示了数字经济背景下“知情-同意”机制面临的深层次困境及其制度根源。核心结论表明：现行机制已陷入形式化合规的窠臼，用户同意的自主性、知情性和具体性被平台权力与技术复杂性所消解。要实现实质性公平，必须推动三重转向——从静态同意转向动态治理，从个体抗争转向制度赋能，从形式审查转向实质评估。研究同时论证了国家安全与个人权益的辩证统一关系：在总体安全观框架下，数据主权构成同意机制运行的边界条件，但国家安全诉求的实现不应以牺牲个人基本权利为代价。通过立法细化的“知情”标准、监管创新的数据信托制度、技术赋能的同意管理工具以及国际协作的规则互认，我国完全可能构建既保障数据安全又尊重个人自主的“同意治理中国方案”。这一路径不仅契合《个人信息保护法》的立法宗旨，更为全球数字治理提供了平衡安全与发展的制度范式。

5.2未来研究方向。随着技术迭代演进，“知情-同意”机制研究亟待开拓新维度：在元宇宙场景中，虚拟身份与现实人格的交叉、脑机接口数据的采集、NFT权属认定等问题，将彻底重构同意的基础逻辑——是否需要建立“数字人格权”框架来承载新型同意？如何设计VR环境下的沉浸式告知界面？这需要跨学科合作构建“元宇宙同意治理学”。量子计算的突破性发展则带来更根本的挑战：现行加密存证技术可能被量子计算机破解，使得同意记录的安全性面临威胁，亟需研发抗量子计算的同意区块链系统。此外，生成式AI引发的“数据来源同意”问题(如训练数据是否需逐项授权)、物联网设备自主决策中的同意代理机制等前沿课题，都要求法学研究与技术发展保持同步进化。这些探索不仅关乎制度完善，更是对“数字文明时代人的主体性如何保障”这一元命题的持续回应。

2024年南京审计大学大学生创新创业 训练计划项目“总体国家安全观下数字经济高质量发展与个人数据安全探究”(2024SX11017)。

[参考文献]

[1]高志宏.大数据时代个人信息保护的理论反思与规则优化[J].学术界,2023(7):122-137.

[2]杨楠.大数据时代我国公民个人信息刑法保护研究[D].江苏:东南大学,2021.

[3]何思源.论个人信息的法律保护[D].湖北:华中师范大学,2020.

[4]覃欣欣.论数据保护法中的知情同意规则--以欧盟《通用数据保护条例》(GDPR)为视角[D].北京:对外经济贸易大学,2020.

[5]李家涵.个人医疗信息知情同意原则的适用困境和完善建议[D].江西:南昌大学,2023.

[6]贺小石.互联网时代个人信息自决权研究[J].编辑学刊,2020(3):42-47.

[7]李艳华.个人数据跨境流动的法律规制与中国方案[D].江苏:南京师范大学,2020.

[8]吴云云.欧盟《通用数据保护条例》中信息自决权研究[D].上海:上海师范大学,2019.

[9]谷丹.大数据时代消费者个人信息保护研究[D].重庆:西南政法大学,2022.

[10]熊嵂杰.我国企业法人数据财产权制度构建研究[D].江西:江西财经大学,2020.

[11]盛小平,郭道胜.科学数据开放共享中的数据安全治理研究[J].图书情报工作,2020,64(22):25-36.

[12]郑志峰.通过设计的个人信息保护[J].华东政法大学学报,2018,21(6):51-66.

[13]朱贝,王传清.我国科学数据共享中的隐私治理探析[J].图书情报工作,2020,64(22):37-47.

[14]OguamanamC.Indigenous peoples,data sovereignty,and self-determination:Current realities and imperatives[J].The African Journal of Information and Communication,2020,26:1-20.

[15]Hummel P, Braun M, Augsberg S, et al. Sovereignty and data sharing[J].ITU Journal on Future and Evolving Technologies,2018,1(2).

作者简介：

刘灌著(2005--),男,汉族,贵州省遵义市播州区人,本科,学生,法学专业(纪检监察方向)。