数据要素流通中的匿名化再识别风险与法律规制

宁伟东，王博琦，时嘉佐，张羽涵，鲍昱含 *
牡丹江医科大学，黑龙江 牡丹江 157011
DOI: 10.61369/TACS.2025080056

摘　　要： 本文旨在探讨数据要素化流通背景下，传统“匿名化”技术所面临的再识别风险及其对现行法律规制体系的挑战。文章首先分析匿名化在数据流通中的法律功能与技术局限，揭示再识别风险的生成机理与具体表现。其次，通过检视我国现行法律框架，指出其存在的“静态认定”与“动态风险”之间的根本矛盾。在此基础上，本文提出应从理念更新与制度重构两个层面予以应对：在理念上，确立“风险控制”为核心、以“场景化评估”为方法的动态安全观；在制度上，构建包含法律定性、标准指引、技术加固与合同约束的协同规制体系，以期在保障数据安全的前提下，有效促进数据要素的合规高效流通。

关 键 词： 数据要素；匿名化；再识别风险；个人信息保护；动态规制

Risk and Legal Regulation of Anonymization Re identification in Data Element Circulation

Ning Weidong, Wang Boqi, Shi Jiazuo, Zhang Yuhan, Bao Yuhan*
Mudanjiang Medical University, Mudanjiang, Heilongjiang 157011

Abstract: This article aims to explore the re identification risks faced by traditional "anonymization" technologies and their challenges to the current legal regulatory system in the context of data elementization circulation. The article first analyzes the legal functions and technical limitations of anonymization in data circulation, revealing the generation mechanism and specific manifestations of re identification risks. Secondly, by examining the current legal framework in China, the fundamental contradiction between "static identification" and "dynamic risk" is pointed out. On this basis, this article proposes that we should respond from two aspects: updating our concepts and restructuring our systems. In terms of concepts, we should establish a dynamic security concept with "risk control" as the core and "scenario based assessment" as the method; In terms of institutional framework, we aim to establish a collaborative regulatory system that includes legal qualification, standard guidance, technical reinforcement, and contractual constraints, in order to effectively promote the compliant and efficient circulation of data elements while ensuring data security.

Keywords: data elements; anonymization; re-identify risks; personal information protection; dynamic regulation

一、引言

随着数字经济时代的全面到来，数据已成为与土地、劳动力、资本、技术并列的关键生产要素。我国“十四五”规划和2035年远景目标纲要明确提出要“激活数据要素潜能”，加快培育数据要素市场[1]。然而，数据要素的高效流通与个人信息保护之间存在着天然的张力：一方面，数据的聚合、流动与共享是实现其经济价值的前提；另一方面，数据中往往包含大量个人信息，其不当处理可能侵犯公民隐私权益[2]。如何平衡数据利用与隐私保护，成为数字时代治理的核心命题。

在这一背景下，匿名化技术被视为调和这一矛盾的关键工具，被赋予了数据流通“安全阀”的期待。通过去除或模糊化数据中的个人标识符，匿名化理论上可以使数据不再属于个人信息范畴，从而在法律上豁免严格的个人信息处理规则，为数据流通扫清障碍。然而，随着大数据技术和人工智能的迅猛发展，这一“安全阀”正面临前所未有的挑战。

匿名化的法律效力建立在“一劳永逸”的安全假设之上——即一旦数据经过适当处理，就永久无法识别到特定个人。然而，这一假设正被日益强大的再识别技术所打破。研究表明，即使是最严格的匿名化处理，也可能通过与其他数据集的交叉验证、背景知识攻击或高级算法推断而实现再识别。重新审视匿名化的法律效力与规制路径，已成为数据要素市场健康发展的核心议题。

本文将遵循“风险揭示—规制困境—路径构建”的逻辑展开分析。首先，深入剖析匿名化再识别风险的本质、生成机理与具

基金项目：创业实践项目 项目编号 S202510229076S
作者简介：宁伟东（1982-），男，硕士研究生，副教授，研究方向：管理科学与工程，卫生管理。
通讯作者：鲍昱含（2000-），女，汉族，山东省潍坊市人，研究生在读，研究方向：临床医学，数据管理。

体表现；其次，系统检视我国现行法律规制体系在应对这一风险时存在的不足与困境；最后，基于风险控制理念和场景化评估方法，提出系统化的法律规制完善建议，以期在保障数据安全的前提下，有效促进数据要素的合规高效流通。

二、匿名化的法律功能与技术脆弱性

在我国《个人信息保护法》第73条中，匿名化被定义为“个人信息经过处理无法识别特定自然人且不能复原的过程”[3]。这一定义赋予了匿名化特殊的法律地位：经过匿名化处理的数据不再属于个人信息范畴，其处理可以豁免《个人信息保护法》中关于个人信息处理的各项规则限制。这一“安全港”制度设计，实质上为数据要素流通提供了一条法律上的“绿色通道”。

但当前的匿名化技术存在技术局限和被再识别的风险。传统匿名化技术主要包括泛化（将精确值替换为范围值）、抑制（删除某些属性或记录）和数据合成（生成统计特性相似的合成数据）等方法[4]。这些技术在单一数据集环境下确实能够有效降低再识别风险，但在大数据时代却面临严峻挑战。一方面，为保持数据效用，匿名化处理往往不能过度泛化或抑制，这保留了潜在的再识别线索；另一方面，通过数据关联和背景知识等算法攻击，可以从数据分布中推断出敏感信息，进而泄露原始数据。匿名化规制面临的核心矛盾在于，法律上对匿名化的认定是静态的、绝对的，即一旦数据被认定为匿名化，就永久豁免个人信息保护规则；而技术上，再识别风险是动态的、概率化的，随着外部数据环境的变化和攻击技术的进步而不断演变。这种静态与动态之间的矛盾，构成了所有规制困境的总根源。这种法律与技术之间的认知鸿沟，使得现行规制体系难以有效应对大数据时代的隐私挑战。

三、我国现行法律规制的检视与困境

我国现行法律体系中，《网络安全法》《数据安全法》和《个人信息保护法》均对数据匿名化、去标识化作出了原则性规定[5]。《个人信息保护法》第73条明确区分了匿名化与去标识化两个概念，赋予前者完全豁免个人信息保护规则的法律效果，而后者仍需遵守部分个人信息处理规则[6]。这一区分体现了立法者对数据流通与隐私保护的平衡考量。然而，现行规定仍存在明显不足：一是标准缺失，二是责任划分不清，三是监管逻辑滞后。

“无法识别特定自然人且不能复原”这一法律标准在实践中面临解释困境。何为“无法识别”，是指技术上不可能实现，还是成本过高而不具可行性。何为“不能复原”，是指绝对不可逆，还是在合理成本范围内不可行。这些问题缺乏明确的技术标准和司法认定准则，导致数据处理者难以准确评估自身行为的法律风险。一旦“匿名化”数据被再识别，原处理者、流通平台、再识别行为实施者之间的法律责任如何划分，现行法规定不清。原处理者是否应对后续的再识别结果负责，如果负责，其责任边界在哪里；流通平台是否应承担审核义务；再识别行为实施者应承担何种法律后果。这些责任分配问题直接影响数据处理者的行为预期和合规成本。而且，当前监管侧重于事前定性（即判断数据是否构成匿名化），而非对流通全过程的动态风险监测与管理。这种静态监管模式难以应对大数据时代的动态风险，既可能因过度严格而阻碍数据流通，也可能因过于宽松而无法有效保护隐私。上述规制困境若得不到有效的改善将不利于数据要素市场的规范化发展。

四、规制理念的更新

面对匿名化技术的固有局限，规制理念必须实现根本性转变：从追求绝对安全转向风险控制。这意味着承认绝对匿名在技术上的不可能性，将规制目标从消除风险调整为管理并控制风险至可接受的水平。这一理念转变并非降低保护标准，而是使法律规制更加符合技术现实，从而实现更有效的保护。风险基础路径的核心是概率化思维：不再将匿名化视为非此即彼的二元状态，而是承认其存在于从完全可识别到完全不可识别的连续谱上，规制任务就是将风险控制在特定场景下可接受的范围内。

贯彻“场景化评估”方法。匿名化效果和再识别风险的高低，依赖于数据的使用场景、接收方能力、潜在危害等因素。因此，规制必须摒弃“一刀切”的静态认定模式，要求结合具体流通场景进行风险评估。通过场景化评估，可以实现规制资源的合理配置：对高风险场景施加更严格的保护要求，对低风险场景则允许相对灵活的数据利用，从而在保护隐私与促进数据利用之间取得动态平衡。

五、构建面向再识别风险的协同法律规制体系

基于风险控制理念和场景化评估方法，本文提出一个多层次、工具协同的规制框架，以有效应对匿名化数据的再识别风险。首先，从法律层面明确责任框架与动态义务。通过司法解释或指南，将“匿名化”重新界定为“经评估，在特定场景下再识别风险处于可接受水平的数据状态”。这一定义将匿名化从静态概念转变为动态概念，强调其场景依赖性和风险相对性。同时，应明确“可接受水平”的判断标准，如再识别概率低于某一阈值（如0.1%），或再识别成本高于某一水平（如100万元）等具体指标。设定持续的风险管理义务，要求匿名化数据处理者在数据流通后，仍负有合理的监控义务，包括关注相关技术发展可能带来的新风险、监测外部数据环境变化（如新的公开数据集发布）、以及定期重新评估数据状态等。这种持续义务能够有效应对风险的动态演变特性。

其次，由监管部门提供操作指引与实施保障。在现有国家标准基础上，制定分行业（如医疗、金融、交通）、分数据类型（如健康数据、金融数据、轨迹数据）的匿名化与再识别风险评估实施指南。这些指南应包含具体的技术方法、评估流程、风险阈值和最佳实践案例，为数据处理者提供可操作的操作指引。推行“认证与审计”机制，鼓励引入第三方专业机构对匿名化方案

和风险控制措施进行合规认证与定期审计，作为数据流通的“信用背书”。认证内容应包括匿名化技术的适当性、场景评估的全面性、风险控制措施的有效性等。审计则应定期进行，确保持续合规。政府应通过税收优惠、研发补贴等方式鼓励企业采用先进技术，同时制定相关技术标准和应用指南。最后，要鼓励采用隐私增强技术。倡导在匿名化基础上，综合运用差分隐私、联邦学习、安全多方计算等新一代隐私增强技术（PETs），从技术根源上降低再识别风险。差分隐私通过添加可控噪声提供数学上的隐私保证；联邦学习允许模型训练而不共享原始数据；安全多方计算则支持在不解密数据的情况下进行联合计算。这些技术能够实现“数据可用不可见”，从根本上缓解再识别风险。

六、结论

数据要素的流通必须在安全与发展之间寻得动态平衡。面对匿名化数据的再识别风险，固守僵化的法律定义已不合时宜。本文主张，我国应果断进行规制理念的更新，在法律上承认风险的动态性，并在制度上构建一个以“风险控制”为核心，法律定性、标准指引、技术加固、合同约束四维协同的规制体系。

这一体系通过重新解释匿名化概念、设定持续风险管理义务、完善技术标准、推广隐私增强技术和强化合同治理，能够有效应对大数据时代的隐私挑战，在保障个人信息权益的同时，充分释放数据要素的经济价值。唯有如此，才能为数据要素的安全、合规、高效流通提供坚实的制度保障，真正实现数字经济的可持续发展。

参考文献

[1] 孙光林，凌真诚，艾永芳 . 数据市场化促进数据要素价值释放的理论逻辑、现实困境与优化路径 [J/OL]. 西南金融，1-10[2025-12-07].https://link.cnki.net/urlid/51.1587.F.20251125.1309.014.

[2] 苏成慧 . 信息处理者安全保障义务的体系阐释 [J/OL]. 河北法学，2026,(01):120-138[2025-12-07].https://doi.org/10.16494/j.cnki.1002-3933.2026.01.007.

[3]Yogi K M，Chakravarthy A .A novel user centric privacy mechanism in cyber physical system[J].Computers & Security,2025,149104163-104163.DOI:10.1016/J.COSE.2024.104163.

[4] 秦倩 . 个人信息保护的权利基础探析 [J]. 重庆大学学报（社会科学版），2023,29(04):203-215.

[5] 陈姿君 . 行政机关采集人脸信息活动的法治因应 [J]. 行政法学研究，2023,(03):153-164.

[6]Miyaji A，Watanabe K，Takano Y，et al.A Privacy-Preserving Distributed Medical Data Integration Security System for Accuracy Assessment of Cancer Screening: Development Study of Novel Data Integration System[J].JMIR Medical Informatics,2022,10(12):e38922-.DOI:10.2196/38922.

