法学与社会治理学刊
2026 Vol. 1, No.1，ISSN 3154-746X

“形式合规，实质宰制”——平台企业数据匿名化的法律规制盲区与治理重构

郑先锋

重庆师范大学

通讯作者*：郑先锋　E-mail：37884683@qq.com

论文信息

关键字

数据匿名化；形式合规；算法宰制；剩余风险；协同治理

摘要

数据匿名化被视为平衡数据利用与个人信息保护的关键制度工具。《个人信息保护法》第 4 条将匿名化信息排除在“个人信息”范畴之外，赋予其法律上的“豁免”地位。然而，这一制度设计在实践中已产生严重异化：平台企业通过技术形式上的匿名化处理规避法定的告知同意与安全保障义务，在“合法”外衣下实现对海量用户数据的实质性支配，形成“形式合规、实质宰制”的治理悖论。本文揭示匿名化的技术标准与法律标准之间的结构性鸿沟，分析平台企业利用匿名化实施差异化定价、算法操纵与市场支配地位滥用的典型表现，并从《个人信息保护法》的豁免条款、反垄断法的适用困境及剩余风险评估机制的阙漏三个维度剖析现行规制盲区。在此基础上，提出技术—制度—市场三位一体的治理重构方案，包括建立匿名化效果认证与动态风险评估机制、出台场景化的匿名化实操细则、推行强制第三方审计制度与用户数据可携带权保障。本文主张打破“匿名化即免责”的法律幻觉，推动数据治理从形式合规迈向实质治理。

"Formal compliance, substantive dominance" - Legal Regulatory Blind Spots and Governance Reconstruction of Data Anonymization in Platform Enterprises

ARTICLE INFO

Keywords

Data anonymization

Formal compliance;

Algorithmic

Abstract

Data anonymization is regarded as a key institutional tool for balancing data utilization and personal information protection. Article 4 of the Personal Information Protection Law excludes anonymized information from the category of "personal information" and grants it a legal "exemption" status. However, this institutional design has undergone serious distortion in practice: platform enterprises evade the legal obligations of notification and consent as well as security guarantees through technical anonymization, and achieve substantive control over

Citation：Zheng, X. F. (2026). “形式合规，实质宰制”——平台企业数据匿名化的法律规制盲区与治理重构 [“Formal compliance, substantive dominance" - Legal Regulatory Blind Spots and Governance Reconstruction of Data Anonymization in Platform Enterprises]. *法学与社会治理学刊*, 1(1), 16–25.

https://doi.org/10.64744/law.2026.265.

dominance
Residual risk
Collaborative governance

massive user data under the guise of "legality", creating a governance paradox of "formal compliance but substantive dominance". This article reveals the structural gap between the technical standards and legal standards of anonymization, analyzes the typical manifestations of platform enterprises using anonymization to implement differentiated pricing, algorithmic manipulation, and abuse of dominant market position, and dissects the current regulatory blind spots from three dimensions: the exemption provisions of the Personal Information Protection Law, the application predicament of the Anti-Monopoly Law, and the deficiencies in the residual risk assessment mechanism. On this basis, a three-in-one governance reconstruction plan of technology, system and market is proposed, including establishing a mechanism for authenticating the effect of anonymization and dynamic risk assessment, introducing scenario-based practical operation details for anonymization, implementing a mandatory third-party auditing system and ensuring the right to carry user data. This article advocates breaking the legal illusion that "anonymization means exemption from liability" and promoting data governance to move from formal compliance to substantive governance.

一、引言

（一）数据匿名化的法律定位：平衡数据利用与个人信息保护的“安全港”

在数字经济时代，个人数据已成为驱动平台经济发展的核心生产要素。如何在充分挖掘数据价值的同时保障个人信息安全，是数据治理领域的基本矛盾。数据匿名化制度正是在这一张力中被寄予厚望的制度工具——通过对个人信息进行技术处理，使其无法识别特定自然人且不能复原，从而在保护个人隐私的前提下释放数据的商业与科研价值。《个人信息保护法》第 4 条明确规定，“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。这一规定意味着，经匿名化处理的信息在法律上被彻底排除在“个人信息”的范畴之外，不再受《个人信息保护法》所规定的告知同意、安全保障、权利行使等一系列规则的约束。

从制度设计的初衷来看，匿名化充当了数据利用与个人信息保护之间的“安全港”：企业通过对数据进行匿名化处理，可以合法地对其加以利用而不必负担沉重的合规义务，个人隐私也因匿名化而得到保护。这一制度安排在理论上实现了效率与安全的精妙平衡。

（二）问题提出：实践中匿名化沦为“形式合规”，平台借此实现“实质宰制”

然而，匿名化制度在实践中正遭遇严重的异化。大量平台企业在名义上对用户数据进行“匿名化”处理，以证明其数据处理行为符合法律规定，从而规避告知同意义务、最小化原则等核心合规要求。但事实上，这些所谓“匿名化”的数据在技术上远未达到真正“不可识别”且“不能复原”的标准。当数据被用于用户画像、个性化推荐、差异化定价等商业场景时，所谓的“匿名”往往只是一个法律修辞，而非实质性的隐私保障。

更值得警惕的是，平台企业借助这一制度漏洞，在“合法合规”的外衣下实现了对用户行为的深度掌控与实质性支配——即本文所称的“实质宰制”。平台不仅通过匿名化数据构

建起精密的用户画像，还借此实施大数据杀熟、算法操纵与市场支配地位滥用等行为。这种“形式合规、实质宰制”的治理悖论，构成了当前数据匿名化法律规制的核心盲区。

（三）核心概念界定：“算法宰制”与“形式合规”

“算法宰制”是指平台企业依托算法技术对用户、商户与劳动者形成系统性控制的结构性权力状态。这种宰制并非通过传统的强制手段实现，而是以“技术中立”为名，通过算法排序、流量分发、价格机制等隐性方式操控资源配置与行为激励，造成信息不对称、权力不对等和行为难预测的结构性失衡。

“形式合规”则指企业在数据处理活动中仅仅满足法律文本的最低形式要求（如履行表面上的匿名化程序、取得形式上的用户同意），却并未真正实现法律所追求的实质目标（如切实保护个人信息权益、保障数据处理行为的公平透明）。形式合规的实质是合规义务的形式化、空心化。

（四）研究方法与结构

本文采用规范分析与实证分析相结合的研究方法，综合运用法律条文分析、技术原理阐释、典型案件梳理与比较法研究，系统考察数据匿名化法律规制的盲区与重构路径。文章结构如下：第二章分析匿名化技术标准与法律标准之间的鸿沟；第三章揭示平台企业利用匿名化实施“实质宰制”的典型表现；第四章从三个维度剖析现行规制盲区；第五章提出技术—制度—市场三位一体的治理重构方案；第六章为结论。

二、数据匿名化的技术标准与法律标准之鸿沟

（一）技术上的匿名化方法：K-匿名、差分隐私、泛化等

数据匿名化在技术层面是指通过一系列数据处理技术，降低数据与个人信息主体之间的关联程度，使其无法识别特定自然人且不能复原。当前主流的匿名化技术包括泛化、抑制、扰动、K-匿名、L-多样性、T-接近性及差分隐私等。

K-匿名模型要求数据集中的每条记录与至少 K-1 条其他记录在准标识符上不可区分，从而阻断通过准标识符链接识别个体的攻击路径。然而，K-匿名模型无法抵御同质化攻击与背景知识攻击，由此催生了 L-多样性与 T-接近性等增强模型。差分隐私则通过向查询结果中添加校准噪声，确保攻击者无法通过对比查询结果的差异来推断某条记录是否在数据集中。2025 年 8 月，全国网络安全标准化技术委员会公布的《数据安全技术 个人信息匿名

化处理指南及评价方法》征求意见稿，系统引入了 K-匿名/L-多样性/T-接近性/差分隐私等隐私模型，并规定了泛化、抑制、分桶、扰动、微聚合、合成等技术机制，同时要求通过对抗性测试和不能复原性核验对匿名化效果进行验证。

（二）法律上的匿名化定义：《个人信息保护法》第4条及相关释义

在法律层面，匿名化的定义远较技术层面简洁。《个人信息保护法》第 73 条将“匿名化”界定为“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”。与“去标识化”（即在不借助额外信息的情况下无法识别特定自然人，但仍可能结合其他信息加以识别）不同，匿名化要求绝对的、不可逆转的不可识别性。

这一法律定义内含两个核心要件：其一是“无法识别”，即从该信息本身无法识别或关联到特定自然人；其二是“不能复原”，即处理后的信息不能被恢复为原始个人信息。然而，这两个要件在法律上均缺乏量化标准和可操作的判定依据，为企业规避合规义务留下了巨大空间。

（三）标准不一致导致的合规漏洞：技术上“匿名”但法律上可重识别

技术标准与法律标准之间的鸿沟是匿名化制度运行中最为根本的结构性矛盾。技术上的匿名化处理往往是一种概率性、场景依赖的保护措施——在特定攻击模型和假设条件下达到一定安全阈值即可视为“匿名”，但这绝不意味着该数据在法律意义上真正实现了“无法识别且不能复原”。而法律上的匿名化标准要求的是一种绝对的、跨越一切场景和攻击模型的不可识别性，这在技术上是极其困难的，甚至可以说在大多数实际应用中是不可能达到的。

这一鸿沟导致了典型的“合规漏洞”：企业按照当前主流技术标准对数据进行了匿名化处理，在形式上满足了合规要求，从而主张《个人信息保护法》第 4 条的豁免适用。然而，这些数据实际上仍具有被重识别的潜在风险——尤其是在平台拥有多源数据并具备强大算力与关联分析能力的情况下，这种风险更加显著。企业恰恰利用了技术与法律标准之间的“模糊地带”，在“匿名化”的盾牌下继续实施对个人数据的实质性支配。

三、平台企业以匿名化实施“实质宰制”的典型表现

（一）以匿名化为名收集海量数据，规避告知同意义务

数据匿名化制度的核心豁免在于：经匿名化处理的信息不再属于“个人信息”，因此其

收集和处理不再需要取得用户同意。这一制度逻辑在实践中被平台企业广泛利用——企业往往在收集用户数据时即宣称将进行匿名化处理，从而主张无需履行告知同意义务，在收集环节即可合法地获取海量用户数据。

然而，实践中大量平台在收集环节并未真正进行有效的匿名化处理，即便进行了初步处理，其技术强度也远不足以达到“无法识别且不能复原”的标准。最高人民法院 2025 年 8 月发布的指导性案例 265 号即揭示了这一问题的典型样态：某科技公司在未征得用户同意的情况下收集用户手机号及用户画像信息，且登录界面未提供“跳过”或“拒绝”选项，被法院认定为“非自愿同意”，构成对个人信息权益的侵害。此案的深层警示在于：如果平台能够以“匿名化”为由绕开告知同意义务，那么此类强制收集行为将在法律上获得“合法化”包装，用户的知情权与选择权将被彻底架空。

（二）匿名化数据的重新识别风险：Netflix奖数据集攻击的警示

匿名化数据被重识别的风险绝非理论推演。2007 年，Narayanan 与 Shmatikov 发表经典论文《How To Break Anonymity of the Netflix Prize Dataset》，对 Netflix 奖数据集的匿名化处理进行了系统攻击。该数据集包含 50 万 Netflix 用户的匿名电影评分记录。两位研究者仅以少量背景知识（如用户对几部电影的评分）为线索，就成功识别出数据集中特定用户的记录，进而挖掘出其政治倾向等敏感信息。

Netflix 案例的核心启示在于：高维数据中的匿名化极其脆弱。用户的偏好、行为轨迹等数据具有高度个性化特征，即便去除了直接标识符（如姓名、身份证号），其独特的行为模式本身即可成为“准标识符”，与其他公开数据源进行关联分析后即可实现重识别。这一风险在平台企业掌握多源、跨场景数据的背景下被急剧放大——平台不仅拥有用户的消费记录，还掌握其地理位置、社交网络、设备信息等多维数据，重识别的能力远超外部攻击者。

（三）利用匿名化数据进行差异化定价、算法操纵与市场支配地位滥用

平台企业利用匿名化数据的“实质宰制”在商业实践中表现得尤为突出。当前的大数据“杀熟”已从早期基于静态身份标签的显性价格差异，演变为依托人工智能、融合多元情境的隐性系统性博弈。在 AI 驱动下，算法不仅能实时捕捉消费者的“瞬时脆弱性”，更能以此精准探测其支付意愿上限。有研究显示，在同等搜索条件下，使用高价值终端设备的用户看到的酒店报价往往比普通设备用户高出 8%至 15%。

平台企业正是通过匿名化数据构建起精密的用户画像和实时定价模型。这些数据虽被宣称为“匿名化”，却足以支撑算法对用户消费能力、需求迫切度、价格弹性的精准推断。在此过程中，用户的行为被转化为可预测、可操纵的变量，算法对用户的控制力从单一价格延伸至搜索排序、流量分配等核心环节。平台经营中潜规则的形成，根源正在于对算法、数据和规则设定的高度垄断，造成信息不对称、权力不对等和行为难预测的结构性失衡。

四、现行规制盲区的法律分析

（一）《个人信息保护法》对匿名化数据的豁免：脱离监管视野

《个人信息保护法》第 4 条将匿名化信息排除在“个人信息”范畴之外，构成了匿名化制度的核心法律依据。这一规定的立法逻辑是：既然匿名化信息无法识别特定个人，也就不存在个人信息权益受侵害的风险，因此无需受个人信息保护规则的约束。这一逻辑在理论推演中成立，但其前提——匿名化在实践中能够真正达到“无法识别且不能复原”——在实践中往往不成立。

当企业依据第 4 条主张匿名化豁免时，监管机构面临两难：一方面，若严格审查企业声称的“匿名化”是否真正符合法定标准，则需要投入巨大的技术评估资源；另一方面，若默认企业的匿名化宣称，则用户数据将实质上脱离《个人信息保护法》的监管视野，形成“脱法地带”。当前监管实践中，后一种倾向更为普遍——大量企业以形式上的匿名化处理规避了实质性的合规审查，匿名化制度从“安全港”异化为“免责金牌”。

（二）反垄断法与反不正当竞争法的适用不足：难以触及“宰制”行为

平台企业利用匿名化数据实施的“实质宰制”，在很大程度上是市场支配地位滥用的表现。然而，现行反垄断法与反不正当竞争法在规制此类行为时存在显著的适用障碍。

首先，举证困难是核心障碍。大数据杀熟等行为具有高度隐蔽性，算法的“黑箱”特性使执法机构难以获取价格歧视、搜索排序操纵等行为的直接证据。即便平台被调查，也可以“算法中立”“匿名化数据不涉及个人信息”为由进行抗辩。2026 年 2 月，市场监管总局对携程集团涉嫌滥用市场支配地位实施垄断行为立案调查，这一事件虽释放了强监管信号，但也凸显出在算法驱动的价格歧视领域，反垄断执法仍面临证据标准与技术评估能力的双重挑战。其次，反垄断法的规制逻辑聚焦于市场竞争秩序而非个人信息权益，对于平台通过匿名化数据实施的“宰制”行为——其侵害对象不仅包括消费者福利，更包括用户的数据自主权与人格尊严——现行反垄断法难以提供充分的保护。

（三）剩余风险评估与处置机制的阙漏：无强制第三方审计

匿名化处理后的数据并非绝对安全，而是存在“剩余风险”——即经过匿名化处理后仍然残留的重识别或信息泄露风险。然而，现行法律框架下缺乏对这一剩余风险的强制性评估与处置机制。

《个人信息保护法》虽要求个人信息处理者采取必要措施保障个人信息安全，但对于匿名化后的数据并未设置专门的剩余风险评估义务。企业在完成匿名化处理后，既无义务向监管机构报告匿名化效果，也无义务接受独立的第三方审计。这种制度阙漏使得匿名化的质量完全依赖于企业的自我评估和自我约束，形成了严重的道德风险。

2025 年施行的《个人信息保护合规审计管理办法》虽引入了个人信息保护合规审计制度，但审计重点涵盖合法性基础审查、匿名化算法可靠性测试等方面。然而，审计频次规则存在一定模糊性：对于处理量低于 1000 万人的企业仅要求“根据自身情况合理确定频次”，可能导致企业面临合规成本不可预测的困境。更关键的是，当前审计制度尚未将匿名化数据的剩余风险评估和动态监测纳入强制性审计范畴，匿名化效果的自我认证仍占据主导地位。

五、治理重构：技术—制度—市场三位一体

（一）技术层面：匿名化效果认证与动态风险评估

重构匿名化治理的第一步，是从技术层面建立可验证、可审计的匿名化效果认证与动态风险评估机制。

2025 年 8 月公布的《数据安全技术 个人信息匿名化处理指南及评价方法》征求意见稿，标志着中国在这一方向迈出了关键一步。该标准提出了对抗性测试与不能复原性核验机制，要求通过模拟潜在攻击者对匿名化数据进行重识别攻击来评估其安全性，并从技术不可逆性、关键辅助材料不可得性与环境不可越权三个维度审查数据不能被复原的程度。

在此基础上，应进一步引入“零信任”理念，摒弃“一次匿名化，终身安全”的静态思维，建立匿名化效果的持续性动态评估机制。匿名化的安全性不是一成不变的——随着技术进步、数据积累和攻击手段的演进，原本安全的匿名化数据可能在新的环境下变得脆弱。因此，企业应当定期对匿名化数据重新进行风险评估，根据评估结果采取补充保护措施或重新进行匿名化处理。

（二）制度层面：场景化的匿名化实操细则

法律对匿名化的定义高度抽象，亟需以法规或规范性文件的形式出台场景化的匿名化实操细则，针对不同敏感度、不同类型的数据设定差异化的匿名化标准。

首先，应当对匿名化的适用场景进行类型化区分。科研、统计分析等非商业性场景可采用相对适中的匿名化标准；而用于商业用户画像、个性化推荐、差异化定价等高风险场景的匿名化数据，则应当适用更高强度的匿名化标准，甚至要求达到“不可重识别”的技术层级。

其次，应当明确匿名化效果的评估主体与责任归属。匿名化“无法识别且不能复原”的判定不应由数据处理者自行完成，而应引入独立的第三方评估机制。对于高风险数据处理活动，应当要求企业就匿名化效果出具第三方认证报告，并将报告提交监管部门备案。

（三）市场层面：强制第三方审计制度、数据可携带权与反重识别投诉机制

在市场层面，应当构建多层次的制度保障体系，形成对平台企业的有效约束。

第一，建立匿名化数据的强制第三方审计制度。当前匿名化效果主要依赖企业自我认证，第三方审计仅在合规审计框架下有限介入。应当明确规定：凡以匿名化为由主张豁免《个人信息保护法》适用义务的企业，必须定期接受独立的第三方匿名化效果审计，审计结果应当向社会公开。第三方审计机构需通过资质认证并受连续审计限制以保障独立性。

第二，强化用户数据可携带权的实现机制。《个人信息保护法》第 45 条确立了数据可携带权，但其在实践中面临格式限制、响应时限等技术性障碍。应当进一步细化相关规定，要求平台企业以机器可读的标准化格式响应用户的数据转移请求，并建立便捷的异议处理渠道。

第三，建立反重识别投诉机制。当用户有合理理由相信其匿名化数据被成功重识别，或其个人信息因匿名化处理不当而遭受侵害时，应当有权向数据处理者提出投诉，并享有向监管机构申诉和向人民法院提起诉讼的救济途径。这一机制将倒逼企业提高匿名化处理的质量，形成有效的市场约束。

六、结论

数据匿名化制度的初衷，是在数据利用与个人信息保护之间建立一座“安全港”。然而，当技术与法律标准的鸿沟被平台企业利用为规避合规义务的制度缝隙，当形式上的匿名化

处理成为“实质宰制”的合法外衣，这一制度便走向了其初衷的反面。

本文的分析表明，匿名化制度的异化根源于三个结构性缺陷：匿名化的技术标准与法律标准之间的规范鸿沟，使企业得以在“技术上匿名”与“法律上可重识别”之间进行制度套利；《个人信息保护法》对匿名化信息的绝对豁免，使用户数据在名义上脱离监管视野；剩余风险评估与处置机制的阙漏，使匿名化质量完全依赖于企业的自我约束，形成了严重的道德风险。

打破“匿名化即免责”的法律幻觉，必须从技术、制度与市场三个维度协同推进治理重构。在技术层面，建立匿名化效果的认证标准与动态风险评估机制，引入零信任理念实现持续性安全监控；在制度层面，出台场景化的匿名化实操细则，区分不同敏感度与不同用途的数据设定差异化标准；在市场层面，推行强制第三方审计制度，强化用户数据可携带权保障，建立反重识别投诉与救济机制。

数据匿名化的治理最终要从“形式合规”走向“实质治理”。这意味着我们不能满足于企业提交的匿名化合规声明，而应当追问：匿名化是否真正达到了“无法识别且不能复原”的法定标准？匿名化数据是否被用于损害用户权益的商业实践？用户的知情权、选择权与救济权是否得到了实质性的保障？只有在全生命周期监管框架下真正回答这些问题，数据匿名化才能回归其作为“安全港”的制度初心，在释放数据价值的同时切实保障个人信息权益。

参考文献

[1] 中华人民共和国个人信息保护法（2021 年 8 月 20 日第十三届全国人民代表大会常务委员会第三十次会议通过）.
[2] 全国网络安全标准化技术委员会. 数据安全技术 个人信息匿名化处理指南及评价方法（征求意见稿）. 2025 年 8 月.
[3] 全国网络安全标准化技术委员会. 个人信息保护 个人信息匿名化指南（征求意见稿）. 2025 年 11 月.
[4] 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. 2025 年 8 月.
[5] Narayanan A, Shmatikov V. How To Break Anonymity of the Netflix Prize Data set[J]. arXiv:cs/0610105, 2006.
[6] 王福春， 付艺轩， 王昱雯， 等. 企业个人信息保护合规审计的实践与挑战[J]. 赣商学院， 2025.
[7] 刘诚. 算法“杀熟”需多元共治[N]. 上海证券报， 2026-02-28.
[8] 平台企业经营中的潜规则现象梳理及建议[N]. 贵州法治报， 2025-09-15.

[9]个保法颁布后企业数据“脱敏”处理的探讨[EB/OL]. 2021-09-23.
[10] 汉盛法评. 数据交易合规系列研究之十五——禁止交易的个人信息探析[EB/OL]. 2022-07-04.
[11] 北京市京师（西安）律师事务所. “同意”的陷阱：从无效同意案例，谈企业如何获取有效的用户授权？[EB/OL]. 2025-12-12.
[12] 夏庆锋. 个人信息匿名化制度的反思与改进[J]. 财经法学， 2024(5).
[13] 赵精武. 个人信息匿名化的理论基础与制度建构[J]. 中外法学， 2024(2).
[14] 何昊洋. 大数据杀熟背后的平台私权力及其法律矫正[J]. 重庆大学学报（社会科学版）， 2023, 29(6): 220-232. DOI: 10.11835/j.issn.1008-5831.fx.2023.08.003.
[15] 陈灿祁. 平台滥用算法权力的法律规制[J]. 湖南科技大学学报（社会科学版）， 2023, 26(06): 154-161. DOI: 10.13582/j.cnki.1672-7835.2023.06.021.
[16] 林北征. 个人信息匿名化概括式立法的困境与完善[J/OL]. 2025. https://www.aisixiang.com/data/159537.html.
[17] Narayanan A, Shmatikov V. Robust De-anonymization of Large Sparse Datasets[C]//2008 IEEE Symposium on Security and Privacy (SP 2008). IEEE， 2008: 111-125.
[18] Leerssen P. Outside the Black Box: From Algorithmic Transparency to Platform Observability in the Digital Services Act[J]. Weizenbaum Journal of the Digital Society， 2024, 4(2). DOI: 10.34669/wi.wjds/4.2.3.
[19] EDPB. Report on Stakeholder Event on Anonymisation and Pseudonymisation [R]. 2026-02-18.