财经法学 No. 4，2024
pp. 160 - 177

复活僵尸法条：个人信息匿名化制度的再造

许　可*

内容提要：《个人信息保护法》第 4 条第 1 款后段将“匿名化信息”排除在个人信息之外，可称为意在数据流通利用的“匿名化条款”。但实施以来，该条款始终存而不用，以至于沦为僵尸法条，成为数据要素市场的最大窒碍之一。既有理论尽管已经充分认识到其病因在于零风险匿名化的预设，但由于缺乏对可接受风险的精确刻画和系统性的规范指引，有解释力而无立起沉疴之力。通过将匿名化信息再利用的风险类型化为系统风险、操作风险、剩余风险，基于匿名化设计的“推定匿名”、基于匿名化条款解释的“判定匿名”、基于匿名化合规的“信任匿名”的同心圆结构渐次形成，不但分别化解了个人信息处理者、监管机构、用户的三重忧虑，而且融技术与法律、过程与结果、场景与系统、数据价值与个人权益于一炉。借此，匿名化条款得以复活，一套操作性和规范性兼备的中国匿名化制度亦由此涅槃重生。

关键词：个人信息　匿名化　推定匿名　判定匿名　相对匿名

沿袭《中华人民共和国网络安全法》第 42 条的“但书”，《中华人民共和国个人信息保护法》（以下简称《个保法》）第 4 条第 1 款后段将“匿名化处理后的信息”排除在“个人信息”之外，从而就“匿名化信息是否属于个人信息”这一争议问题，〔1〕作出明确的立法决断。然而，《个保法》实施以来，该等意在鼓励数据流通利用的条款却几乎从未发挥作用，以至于沦为“徒有法条之形，却毫无生命迹象”的“僵尸法条”，〔2〕成为当前推动数据流通复用、发挥数据要素乘数效应的重大窒碍之一。为此，本文试图把脉既有理论方案，探究匿名化条款的真正病灶，辩证诊治匿名化的三重风险，构造出多层次匿名化的同心圆架构，以期化解个人信息处理者、用户、监管

* 许可，对外经济贸易大学法学院副教授。

本文为国家社科基金重大项目“企业数据安全治理的关键机制研究”（22&ZD147）、国家社科基金一般项目“数据财产权的模块理论及其制度建构研究”（22BFX080）的阶段性成果。

〔1〕 参见丁晓东：《论个人信息概念的不确定性及其法律应对》，载《比较法研究》2022 年第 5 期。

〔2〕 参见葛云松：《物权法的扯淡与认真：评〈物权法草案〉第四、五章》，载《中外法学》2006 年第 1 期。

机构的心疾，最终不负《个保法》的良法美意。

一、匿名化制度的同心圆架构：三重风险与三层匿名

为激活匿名化条款，近年来，学界相继提出“相对匿名化”“动态匿名化”“功能性匿名化”“主观匿名化”“数据关系匿名化”诸多学说。其中，“相对匿名化”主张只要将特定场景下再识别风险控制在“可接受水平”（acceptable level）就构成有效匿名，而不要求风险完全消除。〔2〕“动态匿名化”指出匿名化是一时一地的，并不存在一劳永逸的措施。“功能性匿名化”认为匿名化的关键不在于信息本身，而是被信息和信息环境共同决定的函数。〔3〕“主观匿名化”试图将“世界上一切人采取各种方法均无法再识别”的绝对标准转化为“特定人采取合理可能的方法难以再识别”的相对标准。“数据关系匿名化”则从数据关系理论出发，在保留个人信息一定关联性的同时，隔断显著的横向数据关系，以平衡信息的商业价值和个人权益保护。〔4〕显然，匿名化理论已经粲然大备，但它们能否让匿名化条款起死回生？

（一）匿名化条款僵尸病症的病灶诊断

匿名化条款的病灶不在“腠理”，而在其“心”。详言之，其存而不用的痼疾由三重担心所导致：个人信息处理者既担心匿名化措施难以达到法律要求而无效，又担心标准过高使匿名化信息丧失利用价值；监管机构担心匿名化成为个人信息处理者规避监管的工具；用户担心匿名化是个人信息处理者虚假的承诺。对此，尽管上述理论创新正确认识到“没有任何一种匿名化措施能保证信息完全不被再识别”，但对于满足何种条件才能实现“改进后的匿名化”这一关键问题，既无法提供清晰的行为指引，也难以消解各方忧虑。例如，“相对匿名化”以“可接受水平的再识别风险”为主要论点，可“水平”究竟为何？实践中，针对不同技术、不同场景，往往设置不同风险阈值，目前并不存在统一、明确的量化标准。〔5〕此外还要追问的是：谁来判断“可接受”。是个人信息处理者、用户，还是监管机构？又如，“动态匿名”和“功能性匿名化”通过全面梳理影响匿名化的要素，充分揭示了匿名化的场景性和可变性，可它们主要是描述性的，而非规范性的。再如，“数据关系匿名化”将“风险”限定在“显著关联性的识别”上。可惜的是，该主张的明确性被“关联性”含义的含混性削弱了。正如提倡者所言，关联性既包括因家庭、工作等社会活动所形成的社会关联性，也涵盖基于共同偏好等形成的群体关联性，可其对于如何划定“显著的关联信息”范围却语焉不详。

进而言之，匿名化条款的病灶还在“骨髓”。个人信息处理者、用户、监管机构的心疾在根本上源于匿名化技术和匿名化法律、匿名化过程和匿名化结果、匿名化场景性和匿名化统一性的

〔2〕 参见范为：《大数据时代个人信息定义的再审视》，载《信息安全与通信保密》2016年第10期。

〔3〕 See Mark Elliot, et al., *Functional Anonymization: Personal Data and the Data Environment*, 34 Computer Law & Security Review 204, 221 (2018).

〔4〕 参见赵精武：《个人信息匿名化的理论基础与制度建构》，载《中外法学》2024年第2期。

〔5〕《信息安全技术 个人信息去标识化效果评估指南》未就如何确定风险阈值提供指引。新加坡个人信息保护委员会（Personal Data Protection Commission，PDPC）仅明确使用k-匿名化方案的风险阈值，对于其他技术的风险阈值并未给予明确预设，仅指出“组织应该证明其技术措施与k-匿名化再识别风险相似或更低”。

二元割裂。同样的匿名化，以个人信息处理者为视点，看到的是纷繁的匿名化技术、芜杂的业务场景、系统化的处理过程和精确计算的各种阈值；以用户为视点，看到的是晦涩难懂的匿名化说明和匿名化信息与个人莫名连接；以监管机构为视点，看到的是高度抽象的匿名化规则、统一执法的行政程序和最终暴露的匿名化风险。正如治病应遵循人体系统辨证施治，匿名化条款的诊疗也应诉诸一个集合所有可用方法、策略和工具，协调各种要素和参与者的“个人信息保护系统”(a system of information protection)。〔6〕为此，我们必须仰赖个人信息处理者、用户、监管机构的合力，推动三者相互理解和视域融合（fusion of horizons），促进技术、法律、监管同频共振，最终提炼出操作性与规范性兼备、可预期性与多样性并存、过程导向与结果保障会通的匿名化制度。

（二）基于三重风险的匿名化制度建构

作为一种风险管控措施，匿名化以降低“个人信息再利用风险”为目标。〔7〕不过，在数据海量涌现和算法、算力日新月异的背景下，绝对匿名化无疑是刻舟求剑。更重要的是，信息保护和利用遵循“金发姑娘原则”（goldilocks principle），意即所有匿名化措施都是以信息损失为代价，过于苛刻的匿名化必将导致信息价值损失过巨，以至于得不偿失。〔8〕正因如此，人们逐渐将“处理者匿名化义务有限性”和“国家监管责任有限性”作为匿名化制度的默认前提。承认“有限”不难，难的是“限度”为何。既有理论之所以陷入“理不屈但词穷”的窘境，恰恰在于宏观理念与微观实践的鸿沟。为此，本文试图从类型化风险出发，设置与此相称的“风险容量”(risk appetite)，〔9〕以期作为锚定各方行为边界的刻度。

基于风险后果和发生概率的乘积，个人信息再利用风险由大到小地类型化为“系统风险”“操作风险”“剩余风险”。其中，“系统风险”意指因匿名化措施整体性失效而出现个人信息被大规模不当利用的风险。鉴于该等风险的涉众性和弥散性，一般应采取事前的预防性治理措施，即凭借客观性标准和准入式的红旗规则统一风险防控要求，以防止系统风险的积聚和传导。就此而言，强调“主动而非被动，预防而非补救”的“经由设计的规制”（design-based regulation）恰是因应系统风险的机制设计。〔10〕其秉承代码之法的精神，通过物理设计、技术设定和代码架构，将匿名化标准嵌入其中，成为系统运行的默认规则。一方面，匿名化设计包含了处理者如何行动的剧本，展现了制度刚性并大幅消除了后续法律执行的不确定性；另一方面，匿名化设计亦是处理者的自我约束与自我规制，其可以根据技术发展、差异化场景和多元性目标进行变化和重组，因而具有动态性和适应性（dynamic and adaptive）的特征。但这并不意味着匿名化设计是恣意的，相反，它应当由企业、政府和行业组织共同形塑，并通过由下而上的认可机制在各方之间搭建桥梁，从而与“治理科技”（GovernTech）的多中心治理原则相一致。“操作风险”意指匿名化措施漏洞、内部流程缺陷、人员失误或违规行为等具体因素致使个人信息被不当利用的风险。

〔6〕 参见许可：《个人信息治理的科技之维》，载《东方法学》2021 年第 5 期。

〔7〕 需要说明的是，与常见的“再识别风险”不同，本文使用了更宽泛的“再利用风险”概念。

〔8〕 See K. El Emam & L. Arbuckle, *Anonymizing Health Data*, O'Reilly Media, 2013, p. 185.

〔9〕 参见刘鹏、张崙楠、王力：《基于风险的政府监管：理论发展与实践应用》，载《中国行政管理》2024 年第 3 期。

〔10〕 See Karen Yeung, *Can We Employ Design-Based Regulation While Avoiding Brave New World?* 3 Law, Innovation and Technology 1, 1－29 (2015).

与系统风险不同，操作风险是局部的、分散的场景化风险。就此而言，如果说系统风险体现了“预防型法治”原则，那么操作风险的治理就是“应对型法治”的典型例证。〔11〕质言之，其侧重于个人信息权益损害发生后，通过事后个案认定和处置，引导执法机关和司法机关依法公正处理，对权利人予以救济并对加害人予以精确追责，从而由上而下地管控风险。“剩余风险”意指由匿名化信息所残留的可识别性、难于预见的信息来源和技术革新等不可控因素，所引发的个人信息被不当利用的风险。一般认为，既然剩余风险是采取各种风险防控措施后仍然存在的威胁可能性和潜在影响，那么法律就无需加以干涉。在此意义上，剩余风险构成了国家风险治理的边界。不过，这一观点将治理措施局限在“针对风险的法律规制”之上，而忽略了更多元的治理措施。从政府规制的三分法出发，〔12〕系统风险治理属于事前的“具体行为标准规制”，即以匿名化设计为导向，聚焦于个人信息处理者应当采用的技术标准和实践操作；操作风险治理属于事后的“绩效标准规制”，即以生产结果为导向，明确规定匿名化的效果；而剩余风险治理则属于全链路的“管理型规制”，即以个人信息处理者的决策过程为导向，引导、激励其在宏观组织决策层面提升对剩余风险的学习与适应能力，在微观个体决策层面提升成员执行匿名化方案的能力，〔13〕从而最大程度地缓释风险。

个人信息再利用的三重风险及其治理机制由内而外地构成了三个同心圆，进而与上述三重忧虑的消解相勾连，层层扩展为“推定的匿名”“判定的匿名”“信任的匿名”的匿名化三层结构（见图 1）。

首先，居于中心的是“系统风险”，它不但占据了匿名化风险的最大空间，而且也是个人数据流通复用的最大桎梏。借由公私协作的匿名化设计不但契合了“解铃还须系铃人”的技术优先思路，〔14〕而且能够给个人信息处理者以正反两面的激励。此外，作为一种事前的行为治理，系统风险治理还能够为市场主体划定红线，有助于稳定各方预期并促进数据要素市场的发展。质言之，一旦匿名化设计以间接或直接的方式被国家认可，那么就会产生“推定的匿名”效果。所谓“推定”，即一种根据既定基础事实得出推定事实的规则；而“推定的匿名”则是将“匿名化设计”作为“基础事实”，将“已匿名化的结果”作为“推定事实”的规则。依循证据法的原理，推定匿名是客观举证责任的倒置，个人信息处理者只需证明其采取了合格的匿名化设计，就能获得对匿名化结果的确认，这无疑极大纾解了处理者的忧虑。另一方面，推定的匿名是一种事实推定，其立足于常态联系的盖然性，当然允许他方反驳和提出新的证据予以推翻，不过此时的举证责任已转移给反驳一方承担。〔15〕

其次，从中心向外围拓展，居于中间的是“操作风险”，其既是匿名化风险不可分离的一环，也是国家规制匿名化的关键制度。实践中，有“匿名化设计”之形，却因各种原因致使无“匿名化结果”之实的情形有很多。也正因如此，监管机构对于企业提出的匿名化方案颇为踌躇，担心

〔11〕 参见黄文艺：《论预防型法治》，载《法学研究》2024 年第 2 期。

〔12〕 See Cary Coglianese & DavidLazer，*Management-Based Regulation*：*Prescribing Private Management to AchievePblicGoals*，37 Law and Society Review 691，693－696（2003）.

〔13〕 参见谢尧雯：《个人信息保护企业合规规制的建构》，载《法商研究》2024 年第 2 期。

〔14〕 参见许可：《个人信息治理的科技之维》，载《东方法学》2021 年第 5 期。

〔15〕 参见欧元捷：《民事法律推定的概念检讨》，载《法制与社会发展》2022 年第 4 期。

一旦认可便落入了“匿名化陷阱”，以至于无法后续执法。但正如之前“推定的匿名”所述，匿名化设计是可反驳的推定，若有证据表明其并未实现个人信息匿名化，则处理者仍应遵守个人信息保护相关规则。不过，为维护各方对推定匿名的预期，其推翻应经行政机关或法院依据《个保法》作出判定，我们不妨称之为“判定的匿名”。循此，监管机构得以享有对匿名化设计合法与否的最终决定权，其忧虑自然消弭。

最后，同心圆的边缘是“剩余风险”，其代表了难以预见、难以避免、难以穷尽的匿名化风险。2018 年，美国人口普查局发现，2010 年公布的人口普查统计数据可用来缩小个人信息的可能值范围，从而重构美国 46%（特定条件下 71%）人口的性别、年龄、种族、民族和精细的地理位置。〔16〕故此，个人信息处理者对匿名化信息不得“释放并遗忘”（release and forget），而应继续履行相关合规义务，通过透明化机制保障用户的知情权。同时，监管机构也凭借合规要求，落实强有力的“公共执行”（public enforcement），以弥补剩余风险下私力救济的不足，〔17〕可谓对用户忧虑的积极回应。就此而言，针对剩余风险的匿名机制可称为以用户为导向的“信任的匿名”。

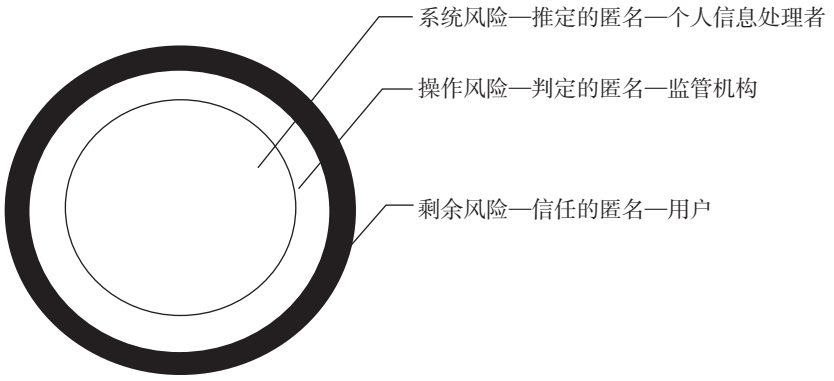

图 1　匿名化制度架构

二、匿名化设计：推定的匿名

（一）匿名化设计的原理

匿名化设计是一套包含策略、硬件、软件、算法、管理措施的复杂机制，一个集密码学、统计学、数据科学、人工智能于一体的系统工程。从流程层面观察，匿名化设计可分为如下步骤：（1）确定匿名化处理对象；（2）对处理对象开展分类分级；（3）梳理匿名化处理的场景；（4）设定匿名化目标；（5）选择匿名化技术及其组合；（6）实施匿名化处理；（7）评估匿名化效果；（8）定期追踪再识别风险。从机制层面观察，匿名化设计首先指向了匿名化管理措施，〔18〕其包括但不限于匿名化组织制度建设、识别和管理数据泄露、持续监控改进、事件应急处置、法律法

〔16〕 See John Abowd, *Stepping-up: The Census Bureau Tries to Be a Good Data Steward in the 21st Century*, Presentation at the Simons Institute for the Theory of Computing, 2019.

〔17〕 参见王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021 年第 5 期。

〔18〕 比如国家市场监督管理总局、国家标准化管理委员会发布的《信息安全技术 匿名化处理指南（草案）》。

规遵从、内外沟通推广；其次指向了“可信执行环境”等匿名化硬件，确保个人信息在隔离和可信的环境中存储、加工和提供，以保证其机密性、完整性、可用性；最后且最重要的是，匿名化设计指向了假名化、泛化、加噪、抑制、差分隐私以及可信密态计算、多方安全计算、联邦学习、同态加密等更广泛的隐私计算技术。鉴于不同匿名化技术各有优劣（见表1），如何根据个人信息性质、使用场景、处理目的设定合理的风险阈值，进而选择最优的技术组合，就成为匿名化设计的关键问题。

表1　　**匿名化技术综述**

技术分类	技术描述	技术效果
假名化	使用基于数学变换生成的假名替换真值	无法保护属性信息，低或中等保密性
泛化	使用范围值代替一般值	难以抵御开放空间里高维关联攻击，低可用性
加噪	在原始信息上添加扰动	
抑制	删除或屏蔽特定信息	
统计	特定类型加工过程，结果只包含统计信息	低通用性
群体标识	采用群体标识和属性代替个人概念信息	低通用性，仅适用于“无需精准个体粒度信息”的场景
隐私计算技术	防范个人信息在计算过程中被他方获取	无法确保输入和输出信息的匿名性

（二）不同场景下匿名化技术的最佳实践

信息利用场景决定着最优匿名化技术的选择。鉴于匿名化和数据交易流通密不可分，在此仅聚焦于“不特定人再利用暨信息公开场景”和“特定人再利用暨信息向第三方提供”这两类场景展开剖析。

在不特定人再利用信息的场景下，“差分隐私”可谓被广泛接受的匿名化最佳实践。作为一种随机分派技术（randomization），差分隐私的核心思想是在公开信息时引入一定的随机性，以确保单个记录对输出结果的影响被限制在一个很小的范围。由此，即使第三方知晓其他所有记录，他们也因单条记录的影响受限，而无法准确获知特定人的信息。本质上，差分隐私是一套严格的算法机制。详言之，给定一个数据库 x，对任意与 x 有且仅有一个数据不同的数据库 y，如果存在定义在 x 和 y 上的随机算法 M，使得对任意的 $S\in M$ 的值域，都有 $\Pr[M(x)\in S]/\Pr[M(y)\in S]\leqslant \exp(\varepsilon)$，则 M 是 ε－差分隐私的算法。〔19〕其中，“隐私预算”ε 对应着区分难度：ε 为0时，完全无法区分；随着 ε 增大，区分的概率相应上升。至于 ε 的数值多少是适当的，可诉诸公开信息的规模、敏感性、安全措施以及潜在攻击者的知识、动机、能力等因素，但一般认为1是理想阈值。〔20〕当前，差分隐私已成功运用于人口普查、数字广告、大型语言模型、高维众包数据等多种场景的匿名化中，并为多国监管机构所认可。美国公布人口普查数据恰是典型一例。由于普查数据包含基层行政区划等多种统计数据，如何防范个人信息的重建攻击成为落实1954年联邦

〔19〕 See Dwork, Cynthia & Aaron Roth, *The Algorithmic Foundations of Differential Privacy*, 9 Foundations and Trends © in Theoretical Computer Science 211 (2014).

〔20〕 See Justin Hsu et al., *Differential Privacy: An Economic Method for Choosing Epsilon*, 2014 IEEE 27th Computer Security Foundations Symposium, IEEE.

《人口普查法》的最大挑战。通过分层添加服从狄利克雷分布的噪声，美国人口普查局利用“集中差分隐私”技术，使得无论特定的个人信息如何取值，均无法从统计中筛选出来，最终实现了信息公开和个人权益保护的双赢。〔21〕

在特定人再利用信息的场景下，“受控匿名”可视为值得高度重视的最佳实践。该方案首先通过 TEE、TECC 等系统安全技术构建具有物理边界的空间，或者凭借密码技术构建逻辑空间。然后，双方或多方将去标识化的个人信息输入上述受控空间内，并切断其与外界开放空间的信息关联。鉴于受控空间处于强管控之下，信息出域被限定在研发调试、结果输出等特定情形下。最后，若出域信息属于统计分析结果、机器学习模型等统计信息，则应保证“不能通过输出信息反推出个体信息”；若出域信息可能属于个人信息，还需要征得个人同意或者具有其他正当性事由。受控匿名的核心思想是将空间内信息与空间外信息相互隔离。由于无法连接外部密钥和开放空间数据，在评估个人信息再利用风险时，仅需结合所有可能进入该空间的数据判断安全威胁，从而不仅大幅降低了再识别的风险，而且保留了信息的可用性。

类似于差分隐私，受控匿名设计因相关个人信息的敏感程度、外部威胁、参与方等因素的不同而有所差异。一般而言，可根据受控空间的特征，分为如下三种类型：（1）基于“主体信任”的受控匿名。其适用于参与方均为善意的场合，即受控空间由参与的一方或多方设立和运营，相关方有能力采取关闭访问控制、人员划分等安全措施。（2）基于“技术信任”的受控匿名。其适用于参与方存在恶意的场合，此时，参与的一方或多方仅且必须依赖技术保障受控空间的安全性，并阻止包括管理员在内的任何人窥探。区别于基于“主体信任”的受控匿名，相关方即便是恶意的，也无法破坏该空间。（3）基于“技术信任”并使用密文运算的受控匿名。其适用于存在恶意敌手攻击的场合，即在高速互联的可信节点集群中，使用密态协议完成目标计算，不但能够阻止包括管理员在内的任何人窥探，又能够缓解侧信道攻击、微架构数据采样攻击、合谋攻击等典型的硬件和协议隐患。据此，即便攻击者打破受控空间，也无法获取个人信息。

无论是差分隐私，还是受控匿名，均旨在将主观、被动、向后看的匿名化法律界定转变为客观、主动、面向未来的匿名化行为标准。凭借可衡量、可审查、可预期的匿名化设计，一方面个人信息处理者得以根据需求和场景来规划、使用、调整匿名化技术，另一方面，国家也能将法律要求转变为技术框架，降低执法成本、减少权力恣意，并为法律与技术的交叉融合开辟了新路。〔22〕

（三）匿名化设计的国家认可机制

最优的匿名化设计能产生推定匿名的法律效果，因而其合法性无法仅由个人信息处理者的自我声明而证成，而必须经由国家一定形式的认可方能获得。容易想到的国家认可方式，无疑是“标准—认证—认可”的三位一体机制。质言之，首先由行业组织推动匿名化设计标准的制定，再由第三方认证机构根据标准对特定个人信息处理者的匿名化设计开展实质评估，最后对符合标准的设计作出认证。在此过程中，国家不但授予认证机构主体资格，还有权全程监督认证过程和

〔21〕 参见朱悦：《差分隐私用于个人信息保护的实践难点及化解方案》，载《信息通信技术与政策》2024 年第 1 期。

〔22〕 See T. Huang & S. Zheng, *Using Differential Privacy to Define Personal, Anonymous, and Pseudonymous Data*, 11 IEEE Access 109225 (2023).

认证结果。〔23〕认证机构能力被公权力统一证明与核验的机制，创制了社会对“认证”的信赖，从而确保了匿名化设计的权威性和正当性。〔24〕然而，由于我国匿名化标准以及具有法定资质的认证机构依然缺失，这一国家认可路径尚未畅通。截至目前，尽管《信息安全技术 个人信息去标识化指南》《信息安全技术 个人信息去标识化效果评估指南》《数据去标识化共享指南》等国家、地方标准相继出台，引入了去标识技术、模型以及常见标识符的去标识化要求，但均未明确“匿名化技术标准”。究其本质，实因去标识和匿名化是一个连续不断的光谱，在行业和监管机构对个人信息再利用风险的刻度欠缺共识的前提下，去标识和匿名化之间的切分线必然难以划定。由此可以理解，正在酝酿的《信息安全技术 匿名化处理指南（草案）》不得不将“个人信息重标识风险接近0”作为匿名化量化标准。但是，这一陈义过高的规则，恐怕会再次落入“僵尸法条”类似的窘境。

在“标准—认证—认可”机制受阻的情形下，“最佳实践—试点示范—认可”机制成为更为有效的进路。所谓“最佳实践”，即建立在证据和价值上的一系列技术、方案、过程、活动组合，其能够对经济和社会发展产生显著的积极影响，并反映了公共机构、私人部门和社会群体的伙伴关系。〔25〕与立足于统一性的“标准”不同，“最佳实践”以多样性的探索为特征，它不强求获得普遍性的共识，而是着眼于实践约束条件和特定场景下达致既定目标的最佳行动模式。正因如此，其远比标准更易形成。就国家而言，最佳实践并不意味着当然的“合法实践”，而更像是一种行业推荐的“应用试点”，只有经过申报和监管机构评选后，才能成为普遍推广的示范技术。在此过程中，监管机构要坚持“设计中立性原则”，〔26〕避免将监管作为手段，偏袒特定匿名化技术或限制其发展，个人信息处理者可以基于“性能标准”，自由选择最适合实现匿名化的设计。这是因为，在一个高度动态的市场中，监管者不应试图挑选技术赢家、阻碍技术创新。另一方面，监管机构应当汲取“沙盒监管”的理念，为经过评选的匿名化设计提供更灵活、有弹性的监管环境和责任豁免机制，〔27〕同时强化“设计试点”和“监管试点”的彼此促进，通过技术创新推动监管创新和法律的同步优化。

三、匿名化条款：判定的匿名

个人信息处理者实施了匿名化措施，但最终被认定失败的例子并不罕见。例如，在2022年意大利数据保护局对Google Analytics的处罚案中，尽管Google Analytics采取了“IP匿名化”

〔23〕 参见张继红：《数据认证：模式选择与应用规范》，载《中国政法大学学报》2021年第2期。

〔24〕 参见许登科：《行政法上认证与验证之制度审视其法理——以德国产品安全法为中心（上）》，载《中正大学法学集刊》2021年第72期。

〔25〕 See Osburn, Joe, Guy Caruso & Wolf Wolfensberger, *The Concept of “Best Practice”: A Brief Overview of Its Meanings, Scope, Uses, and Shortcomings*, 58 International Journal of Disability, Development and Education 213 (2011).

〔26〕 这一概念借鉴了“技术中立性原则”（Technological Neutrality）。See Winston Maxwell & Marc Bourreau, *Technology Neutrality in Internet, Telecoms and Data Protection Regulation*, 1 Computer and Telecommunications Law Review 1 (2014).

〔27〕 参见宋科、傅晓骏：《监管沙盒的国际经验与中国应用——兼论我国“监管试点”与“监管沙盒”的异同》，载《金融监管研究》2021年第9期。

技术，从而在网络运营商发送用户 IP 地址时，遮掩其中的 8 位数（如地址 122.48.54.0 至 122.48.54.255 将被 122.48.54.0 所取代），但数据保护局认为：这种匿名化并不能阻止 Google Analytics 根据其掌握的用户整体信息重新识别用户，事实上，当用户访问其谷歌个人信息，他们的 IP 地址与其他附加信息得以联系起来。〔28〕又如，在 2022 年比利时数据保护局对 Interactive Advertising Bureau Europe（IAB）的处罚案中，〔29〕IAB 开发了“透明度和同意框架”（the transparency and consent framework，TCF），用以捕获用户对“同意管理平台”的响应，即他们是否同意收集和共享个人信息以及是否反对广告商基于正当利益的处理。用户的响应被编码并存储在“T[ransparency] C[onsent] 字符串”中，并与他方共享，以便后者知晓用户的反应。比利时数据保护局认为：虽然 TC 字符串本身是技术信息，并不能直接区分出用户，但其提供了一种标准化的方法来收集和交换来自可确定、已识别或至少可识别的用户的信息。数据保护局进一步指出：如果相关方处理的目的是把个人筛选出来，则可假定其拥有或将拥有能够合理地预期识别信息主体的手段，而此时声称个人是不可识别或匿名化的，不啻自相矛盾。

匿名化措施的失败或源于相关设计并未消除系统风险，或源于操作风险的存在。因此，匿名化设计的认可机制不过是化解风险的第一步，当个人或监管机构确有理由怀疑匿名化的真实效果时，可以在事后通过举报、诉讼、执法检查等法律程序，全面审查个人信息处理者的匿名化设计，并作出维持或推翻的最终判断。不过，为了保护各方的合理信赖，对推定匿名的否定一般不具有对事前处理活动的溯及力，以维持既存的数据流通秩序。与推定匿名以“技术治理”为基础不同，判定匿名有赖于国家机关依法作出的司法判决或行政行为，属于传统的“法律治理”，其落点自然系于法律规则，即对《个保法》第 73 条第 4 项“匿名化，是指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”下“无法识别”“不能复原”“过程”等核心概念的法律解释之上。

（一）“无法识别”的法律解释

基于要素结构化的思路，“无法识别”可以进一步细分为“识别行为”“识别对象”“识别主体”“识别方式”等子概念。

1. 识别行为

从文义解释出发，“识别行为”即辨别、辨认的行为，〔30〕意指根据不同事物的特点，在认识上加以区别，或者根据特点做出判断，以便找出或认定某一对象。据此，对特定自然人的识别，就是根据人的特征，将特定人从人群中“筛出”（single out）。不过，这一解释可能与体系解释存在罅隙。根据《个保法》第 4 条第 1 款中“个人信息—匿名化信息”的二分法，匿名化应当同时考虑个人信息的界定，即“与已识别或者可识别的自然人有关的各种信息”。由此引发的问题是：这里的“无法识别”如何与“不再有关”相协调。对这一问题的回答，还需要重新审视“识别”。法律中“识别”（identify）的首要含义是“证明某人或某种事物的同一性”〔31〕，就此而言，“识别”意味着“相关信息”和“特定自然人”的“同一性”。与文义解释强调“区分”的“筛出”

〔28〕 Garante per la protezione dei dati personali-9782890.

〔29〕 APD/GBA（Belgium）- 21/2022.

〔30〕 参见中国社会科学院语言研究所词典编辑室编：《现代汉语词典》（第 7 版），商务印书馆 2016 年版，第 1185 页。

〔31〕 Bryan A. Garner ed.，*Black's Law Dictionary*，West Group，2009，p. 813.

有异，“同一性”突出了信息内容对“特定自然人”的映射，并借此限缩了含义模糊的“有关”。详言之，相关信息和特定自然人的关联应当是客观的、唯一的和相对稳定的，另一个人具有相同特征的机会为零或接近于零，从而得以正确描摹出现实中某一个人。〔32〕这一突出“个人唯一身份（identity）”的解释，也与目的解释相契合——《个保法》保护的并不是“信息”，而是信息所映射的自然人及其在数字时代身份建构的自主性和完整性。〔33〕

2. 识别对象

基于上述对识别行为的解释，自然人的“身份”成为识别的对象。“身份”并不限于“公民身份”（civil identity），还指向了更广义的“社会身份”和更狭义的“自然身份”。其中，“公民身份”系个人在政治国家中的唯一身份，〔34〕它由出生证明、身份证、护照、户口等资料所组成，涉及个人的法定姓名、出生日期、户籍、国籍、居住地址等特征。公民身份是国家对公民的基础性认证，以此用于公共管理和公共服务。“社会身份”系个人在社会交往、经济活动中呈现的角色、属性和特征，涵盖了：（1）以血缘、婚姻、长期共同生活所形成的亲属、婚姻等法定身份，（2）向熟人、朋友、同事及陌生人展示的“人物设定”；〔35〕（3）个人根据共享的特征、信念、经验，将自己归属于多个社会群体的“成员身份”，如种族、民族、劳动者、消费者、政党成员等。社会身份彰显了个人独特的社会规定性。“自然身份”系个人作为生物体所具有的生理、生物特征和身体动静，主要表现为指纹、声纹、掌纹、耳廓、虹膜、面部特征、步态、行踪轨迹、个人基因等。需要说明的是，本文将个人的内在情感、精神、心理特征、思想世界等排除在“身份”之外。这是因为，如果说“人是社会关系的总和”，那么并未表现于外的种种信息全然属于个人隐私领域，在法律规范上成为隐私权的对象，一般优先于个人信息规范的适用。〔36〕

3. 识别主体

较诸“识别对象”，对“识别主体”的解释分歧更为严重。根据主体范围由广到窄，可以胪列如下：（1）世界上任何一人（anyone in the world）。欧盟在《一般数据保护条例》（GDPR）的序言中指出，判断是否可识别，需考虑包括信息处理者及其他人在内的所有人能否直接或间接识别出特定个人。（2）有心侵入者（motivated intruder）。英国信息专员办公室（Information Commissioner's Office，ICO）将识别主体限定在对信息及其可能揭示的内容感兴趣的人，其拥有合理的搜寻、比对和查验能力，可取得公开可取得的资料，并向别人开展一般性调查，但不具备任何专业知识和先前知识，就此而言，或可称为“社会一般人”。〔37〕（3）信息提供者。日本学界和实务界就识别主体均采“个人信息处理事业基准说”，即处理者将保有的个人信息提供给他

〔32〕 See Nadezhda Purtova, *From Knowing by Name to Targeting: the Meaning of Identification under the GDPR*, 12 International Data Privacy Law 163 (2022).

〔33〕 参见陆青：《数字时代的身份构建及其法律保障：以个人信息保护为中心的思考》，载《法学研究》2021年第5期。

〔34〕 See Leenes, *Ronald: Do they Know Me? Deconstructing Identifiability*, 4 University of Ottawa Law & Technology Journal 135, 140 (2007)

〔35〕 参见曹博：《个人信息可识别性解释路径的反思与重构》，载《行政法学研究》2022年第4期。

〔36〕 参见许可：《权利树：个人信息权益的理论重述》，载《甘肃社会科学》2024年第2期。

〔37〕 See ICO, *Determining What Is Personal Data*, 12 December 2012.

人时，仍以原处理者为准，即该相关信息是否具有可识别性，依信息提供者的条件、技术、处理状况等判断。〔38〕（4）信息接收者。作为促进个人健康信息的流通和分享的机制，美国《健康保险携带和问责法》（HIPAA）统一了电子个人健康信息传输标准，还提出了个人信息去标识化（匿名化）的“专家标准”（expert determination）和“预期接收者”（anticipated recipient）测试，即具有统计学、数据等相关知识和经验的专家确定“预期接收者”单独或与其他合理可获得的信息结合，识别个人的风险非常小，则满足去标识化（匿名化）标准。

不同解释反映出各国不同的取舍：从“世界上任何一人”到“信息接收者”，个人信息保护愈加为数据流动容留更大的空间。当前，数据作为关键生产要素的价值凸显，人工智能亦在以前所未有的方式创新数据使用，个人信息保护和数据流动之间亟待再平衡。事实上，欧盟在 GDPR 之后的《非个人数据自由流动条例》《数据治理法》《数据法》中均鲜明体现了促进数据流动的立法意旨。在 2023 年 SRB v. EDPS 案中，欧盟普通法院将识别主体锚定在“信息接收者”之上，充分反映出这一趋势。〔39〕在该案中，“单一清算委员会”（SRB）将债权人、股东的个人信息提供给德勤公司展开分析，并使用“字母数字代码”（alphanumeric code）取代个人身份信息。欧盟普通法院明确否定了欧洲数据保护监督机构（EDPS）所认为的“没有必要确定传输给德勤的信息是否可以被重新识别，或该等重新识别是否合理可能”，而是援引 Patrick Breyer v. Federal Republic of Germany 案，〔40〕旗帜鲜明地指出：应站在接收者德勤的立场上，确定传输给它的信息是否与“可识别个人”有关。尽管 SRB 持有字母数字代码和识别数据库等额外信息，但没有证据证明德勤曾经或现在有能力解密或倒推身份，因此 SRB 提供的信息属于“匿名化信息”。回到我国，将识别主体限定在信息接收者，有助于消解个人信息提供者依法保存义务和数据流通的法律冲突。〔41〕事实上，《互联网广告匿名化实施指南》第 5.1 条亦明确“采取信息接收者标准”，在没有其他独立管理的额外信息的辅助下无法识别特定自然人的，构成匿名化信息。

4. 识别方式

法律不强人所难。“识别方式”并非要遍历世界上一切可用措施，而是指“合理可能”（reasonably likely）的手段。欧盟法院认为：如果法律禁止识别，或因时间、成本和人力上需要付出不成比例的努力，识别特定主体在实际上不可能，则身份识别的风险在现实中微不足道，从而不构成识别。〔42〕这与我国义务履行以“一般社会观念”为准的原则相契合。例如，大海捞针虽属可能，但需要付出非常不合理的劳力、费用，社会观念上认为履行不能。〔43〕除“事实上的不可能”和“经济上的不可能”外，“法律上的不可能”即被禁止的识别方法（如黑客攻击）亦

〔38〕 参见范姜真微：《匿名加工资料制度之创设———因应大数据时代日本个人资料保护法之新进展》，载《东海大学法学研究》2020 年第 59 期。

〔39〕 See SRB v EDPS（ECLI：EU：T：2023：219）

〔40〕 See Patrick Breyer v. Federal Republic of Germany（Joined Cases C468/10 and C469/10）.

〔41〕《中华人民共和国网络安全法》、《中华人民共和国反洗钱法》、《中华人民共和国证券法》（2019 年修订）、《中华人民共和国电子商务法》、《征信业管理条例》、《互联网信息服务管理办法》（2011 年修订）等法律法规均明确规定了个人信息依法保存义务，即个人信息处理者不得在法定期限内删除或实施匿名化。

〔42〕 参见〔波兰〕马里厄斯·克里奇斯托弗克：《欧盟个人数据保护制度：〈一般数据保护条例〉》，商务印书馆 2023 年版，第 55 页。

〔43〕 参见韩世远：《合同法总论》（第 4 版），法律出版社 2018 年版，第 522 页。

应排除。总之，判断能否识别时，不应抽象地思考可能性，而应立足特定主体，在行业通常技术条件和法律允许范围内，综合分析其可能合理获得的信息和所付出的成本后作出判断。

（二）“不能复原”的法律解释

1. 复原行为

与欧盟强调“不可逆”（irreversible）即“不能被重新识别”有异，我国采用“不能复原”这一表述。〔44〕基于体系解释，“不能复原”有单独存在的意义，其和“无法识别”应区分理解，不可视为同义互文。在比较法解释上，“不能复原”借鉴了《日本个人信息保护法》第2条“无法识别特定个人，并无法复原后的个人信息”。根据该法修正案的官方英文译本，〔45〕“复原”（restore）指向了“原始个人信息和相关识别符号”，所谓“不能复原”，即去标识化后信息不能因技术应用恢复识别符号的原状。循此，我国法下“复原”可理解为通过逆向回溯分解出匿名处理方法，再利用组合、比对将匿名化信息复原成个人信息。举例而言，针对姓名替换为乱码或变换为其他文字排列的匿名信息，将所使用的乱码锁定后，反复排列组合测试出原本姓名。〔46〕

2. 复原对象

尽管复原是对原始个人信息的恢复，但对象未必是全部信息，“实质部分”便为已足。作为个人信息的核心元素，实质部分一旦缺失就会失去信息利用的基本价值。譬如，手机号码的核心部分是第4—11位（所在地区和用户标号），如果仅复原前3位（网络识别号），并无价值。相反，身份证号码每一个号码段均有特殊意义，复原任一部分都可能构成实质性复原。另一方面，尽管处理者不能复原实质部分，但利用其他材料，通过非实质部分推断出实质部分，也可视为复原。需要补充说明的是，如处理者将非实质部分和自身所掌握的其他资料相结合，识别出特定自然人并生成新的个人信息，依然不属于“复原”，因为原始信息并未恢复，这亦是“复原”和“识别”二分的当然之意。不过，此时个人信息处理者应重新获得个人同意或具备《个保法》第13条下的其他正当性事由。但这不必然意味着匿名化失败，因为在某种情形下可被视为“个人信息的重新收集”而非“再识别”。〔47〕

3. 复原主体

与识别主体类似，复原主体亦应是信息接收者。这一见解可见于我国台湾地区的判决。在台北高等行政法院103年度诉更一字第120号判决中，法院认为，尽管“资料保有者仍保有代码、原始识别资料对照表或解密工具而得还原为识别资料，但只要原资料保有者并未将对照表或解密方法等连结工具提供给资料使用者，其释出之资料无法透过该资料与其他公众可得之资料对照、组合、连结而识别出特定个人时，该释出之资料即属无法直接或间接识别之资料”。德国和英国相关学说亦认为：即使提供者仍可复原个人信息，但对于信息接收者难以复原，即可认为已非个

〔44〕 参见谢琳：《大数据时代个人信息边界的界定》，载《学术研究》2019年第3期。

〔45〕 See *Amended Act on the Protection of Personal Information*, availableat www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf, last visited on Feb.15, 2024.

〔46〕 参见范姜真媺：《匿名加工资料制度之创设——因应大数据时代日本个人资料保护法之新进展》，载《东海大学法学研究》2020年第59期。

〔47〕 可参见下文“（三）‘过程’的法律解释”。

人信息，而无个人信息保护之适用。〔48〕

4. 复原方式

基于合理活用个人信息的考量，“复原”一如“识别”，亦凭借社会公众或特定行业（如金融、医疗）的一般能力、手段、技术，借由通常方式进行，费用、时间等投入应与其受益成比例，因而不存在不计成本的复原。与“识别”不同，复原应采同样的匿名化方式或者其他具有同等功能的算法。例如，在删除性别信息的匿名个人信息中，根据购买化妆品的购买记录较多，确定原性别信息为女性，在这一过程中并没有使用之前的匿名化工具，本质上属于无损个人权益的“推断性披露”（inferential disclosure），而非“复原”或 GDPR 下的“推断”（inference），前者系基于数据统计特性，以“高置信度”（high confidence）推断出信息，后者是从个人的一系列属性推断出特定属性，两者切不可同日而语。

（三）“过程”的法律解释

《个保法》第 73 条第 4 项将“过程”作为匿名化的“属”概念，凸显了“过程进路”（process-based approach）的意义。正如计算机科学研究发现的，隐私是分析的输入物与输出物之间的信息关系，而不只是输出物自身的属性。因此，只看结果（输出的信息是否为匿名化的）而轻视过程（是否采取了有效降低个人信息再利用风险的措施）的匿名化制度，无法提供系统性和面向未来的个人信息保护。〔49〕就此而言，“过程”一词可解释为我国对“结果匿名化”的摒弃和对“过程匿名化”的认可。

过程匿名化首先从“绝对匿名”转向了“相对匿名”，从强调“零风险”转向合理控制风险。其次，过程匿名化从最终的“处理状态”转向了动态的“处理流程”，既囊括环境维护、确定目标、技术处理、效果评估和行为控制等步骤，也纳入了上述步骤的实施过程和效果的管理和监测。再次，过程匿名化从单纯的“信息”转向了复杂的“信息场景”，即与信息发生交互并为之提供解释的“数据环境”，包括但并不限于物理基础设施、其他可得的信息、信息处理者及其管理个人信息的各种数据治理工具。〔50〕最后，过程匿名化从狭义的“技术”转向了广义的“系统”，综合考量个人合理的隐私期待、个人信息的数量和敏感程度、接收者及其处理的目的、方式以及访问权限控制等诸多因素。〔51〕基于上述转型，过程匿名化的实施应融技术、规制和权利保护为一体，〔52〕在数据流通利用中秉持如下原则：（1）评估对外提供的个人信息及其敏感程度；（2）根据最小必要原则设定提供个人信息的数量、类型和范围；（3）实施合理、良善的匿名化技术并在必要时采取额外的数据安全措施；（4）制定监测、问责和违约应对计划。〔53〕

---

〔48〕 参见林裕嘉：《公务机关利用去识别化资料之风险评估及法律责任（上）》，载《司法周刊》2017 年第 1852 期。

〔49〕 See Micah Altman et al., *A Principled Approach to Defining Anonymization As Applied to EU Data Protection Law* (May 9, 2022), available at SSRN: https://ssrn.com/abstract=4104748 or http://dx.doi.org/10.2139/ssrn.4104748, last visited on Mar. 2, 2024.

〔50〕 See Mark Elliot, et al., *Functional Anonymization: Personal Data and the Data Environment*, 34 Computer Law & Security Review 204, 221 (2018).

〔51〕 See Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 710 (2015).

〔52〕 See Chris Achatz & Susan Hubbard, *Us vs. Eu Guidelines for De-Identification, Anonymization, and Pseudonymization*, 20 Journal of Internet Law 1, 7 (2017).

〔53〕 See Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 710 (2015).

除上述较为宏观制度设计外，将过程匿名运用于“判定匿名”中，还可得到“阶段性匿名”的微观认识。详言之，一个典型的信息处理过程可以分为“信息输入”“分析使用”“结果输出”三阶段。在判断匿名化与否时，应将各阶段视为彼此区隔的环节，每一环节均应独立认定。以本文第二部分的“受控匿名”为例：在信息输入阶段，信息经过了去标识处理，但仍可结合其他信息识别个人且可复原，并不属于匿名化信息，其输入理应具有合法性基础，遵循正当、合法、必要、诚信原则；在分析使用阶段，鉴于信息被禁锢于受控空间之内，依据空间内的全部信息无法识别个人，同时不能恢复输入之前的个人信息，可认定构成了匿名化处理；在结果输出阶段，信息可能指向个人（如用于个性化推荐、信用评价），也可能不以定位个人为目标（如用于大模型训练和优化）。显然，只有不以定位个人为目标的信息才系匿名化信息。但无论最终输出结果如何，分析使用阶段的匿名化判定均不受其影响。

四、匿名化合规：信任的匿名

如果说“推定的匿名”消除了个人信息处理者的忧虑，“判定的匿名”缓解了监管机构的忧虑，“合规的匿名”则以回应用户的忧虑为依归。在匿名化的剩余风险不可能完全涤除的风险社会中，任何零风险的声称都是神话甚或欺骗。就此而言，匿名化制度不应给公众提供虚假的安慰，而应致力于通过可操作的规则构建用户、个人信息处理者与监管机构之间的信任，进而形成“信任共同体”。这不仅是因为，个人信息权益的本质就是信任，而非个人的控制，〔54〕更重要的是，信任恰是应对不确定、不可控未来的简化策略。〔55〕但，信任并不容易。实践中，为了解决个人信息保护与利用的数字信任危机，个人信息保护法已经发展出多样化的工具体系。〔56〕其中，个人信息处理相关资讯的沟通在信任建构中居于中心位置。质言之，作为持续性关系的产物，信任依托于各方之间的资讯交互。现有研究充分表明：充分、可靠、及时的资讯交流是增进信任的前提，也是风险管理的基础。〔57〕立基于此，以信任匿名为目标的匿名化合规应落脚在匿名化处理的资讯沟通之上。

（一）从“匿名化同意”到“匿名化知情”

用户对于匿名化处理是否享有同意权？欧盟 GDPR 认为，匿名化是对个人信息的加工和变更，亦为个人信息处理活动，理应取得个人同意或具备第 6 条所列其他合法性事由。〔58〕赋予个人对匿名化的决定权看似是对个人权利的最大保障，可事实上，信任始终是双方的事业，试图通

〔54〕 参见〔波兰〕彼得·什托姆普卡：《信任：一种社会学理论》，程胜利译，中华书局 2005 年版，第 32 页。

〔55〕 See Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in the Twenty-First Century*, 69 University of Miami Law Review 559, 559 (2015).

〔56〕 参见许可：《诚信原则：个人信息保护与利用平衡的信任路径》，载《中外法学》2022 年第 5 期。

〔57〕 参见王俊秀、周迎楠、刘晓柳：《信息、信任与信心：风险共同体的建构机制》，载《社会学研究》2020 年第 4 期。

〔58〕 参见〔瑞士〕Maria Cristina Galdarola、Joachim Schrey：《大数据与法律实务指南》，赵彦清、黄俊凯译，元照出版公司 2020 年版，第 182 页。

过“用户赋权—企业担责”的单向路径实现信任，往往事倍功半。〔59〕匿名化作为个人信息的安全保障措施，显著降低了后续处理活动对个人的威胁，又作为数据流通的整体方案，显著提高了处理者和潜在第三方使用数据的利益，且此种利益是真实、具体和明确的，足以构成欧盟 GDPR 下的“正当利益”(legitimate interests)，从而豁免个人同意。在我国法下，则可诉诸《个保法》第 5 条下的“诚信原则”，通过灵活的利益平衡获得匿名化处理的正当性。

匿名化无需个人同意，并不意味着个人无需知情。在《个保法》中，除“紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知”外，知情权不得被克减。这首先因为，知情权是个人自主的基础，在个人信息权益这一权利树中，是催生其他权利生长的“主干”，〔60〕另一方面，知情权不只是“知”的权利，还是“行”的权利，〔61〕是监督个人信息处理者全面履行匿名化承诺和合规义务的权利。循此，用户的匿名化知情权可转化为个人信息处理者的如下义务：

其一，匿名化之前的告知义务。个人信息处理者在进行匿名化之前，应当在隐私政策或个人信息规则中明确告知用户匿名化的目的、方式和处理信息的种类和范围。此外，考虑到用户的疑虑，处理者还应进一步说明：(1) 匿名化的风险以及由此可能产生的后果，特别是，是否计划公开匿名化信息或向其他人披露；(2) 采取了哪些保护措施来最大程度地降低匿名化的风险；(3) 在信息公开的场景中发布匿名化信息的理由，以及基于哪些因素予以权衡。〔62〕例如，Meta 在其隐私政策中逐项罗列了匿名化的范围：(1) 用户的动态和提供的信息；(2) 好友、粉丝和其他联系人的信息；(3) 应用、浏览器和设备的信息；(4) 来自合伙伙伴、供应商和第三方的信息。〔63〕Google 亦明确告知用户匿名化目的和使用的技术。〔64〕遗憾的是，我国处理者少有告知上述信息，而多见豁免的声明。例如，《美团隐私政策》第 3 条规定：“根据法律规定，共享、转让、公开披露经去标识化处理的个人信息，且确保数据接收方无法复原并重新识别个人信息主体的，我们对此类数据的处理将无需另行向您通知并征得您的同意。”〔65〕

其二，匿名化之后的公示义务。由于用户无法参与匿名化处理过程，为确保其知情权，个人信息处理者应当在完成匿名化后，通过网页、邮件或站内消息等方式，公告匿名化的资讯。相关公告应在合理期限内发布，且不得晚于匿名化信息的后续利用或向第三方提供之时。

其三，匿名化信息向第三方提供之前的公示义务。为了让用户知悉匿名化信息的流通和利用

〔59〕 参见许可：《欧盟〈一般数据保护条例〉的周年回顾与反思》，载《电子知识产权》2019 年第 6 期。

〔60〕 参见许可：《权利树：个人信息权益的理论重述》，载《甘肃社会科学》2024 年第 2 期。

〔61〕 参见王锡锌：《滥用知情权的逻辑及展开》，载《法学研究》2017 年第 6 期。

〔62〕 See ICO, *Accountability and Governance in Draft Anonymisation, Pseudonymisation and Privacy Enhancing Technologies Guidance*, Chapter 4.

〔63〕 参见《Meta 隐私权政策》，载 https://www.facebook.com/privacy/policy/?entry_point=facebook_page_footer，最后访问时间：2024 年 3 月 26 日。

〔64〕 参见《Google 隐私权和条款》，载 https://policies.google.com/technologies/anonymization?hl=zh-CN，最后访问时间：2024 年 3 月 27 日。

〔65〕 《美团隐私政策》，载 https://rules-center.meituan.com/rules-detail/2，最后访问时间：2024 年 2 月 26 日。另参见《百度隐私政策总则》第 5 条，载 https://privacy.baidu.com/policy，最后访问时间：2024 年 2 月 26 日。

过程，进而监督其合法利用，个人信息处理者将匿名化信息提供给第三方时，应事先公布相关信息的内容以及提供方式，并同时向第三方明示提供信息为匿名化信息。〔66〕

考虑到匿名化处理和后续信息利用的惯常性和继续性，上述第二项和第三项的公告可以在首次发生时作出，已载明相关期限的，可免除后续的公示义务。

（二）从“禁止再识别”到“再利用的个人信息保护影响评估”

从英国《数据保护法案》（Data Protection Bill）到《加州隐私权法案》（The California Privacy Rights Act），禁止匿名化信息的再识别已成为因应匿名化剩余风险的普遍规则。〔67〕但这并不能打消用户的猜疑，理由简单明了：信息处理活动是一个黑箱，外人难窥究竟。是故，如何取信于人成为禁止再识别义务履行的症结所在。从上述资讯沟通的进路出发，不妨转换思路，将禁止再识别的自证清白义务贯彻于匿名化信息再利用的“个人信息保护影响评估”之上，相关评估结果和报告摘要应向社会和监管机构公开，以期实现风险评估、风险沟通和风险决策的规制闭环。

所谓“个人信息保护影响评估”，是指通过评估个人信息处理目的、处理方式等是否合法、正当、必要、诚信，对个人权益的影响及安全风险，所采取保护措施是否有效及与风险的适应程度等，判断其对个人权益的影响程度及风险控制有效性的过程。〔68〕作为风险预警机制和事前的合规检验，它为各方提供一种风险发现方法，帮助个人信息处理者在项目实际处理之前实施预防措施和专项保护措施，如果风险影响非常严重且无法预防，项目将被终止。自 1995 年《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC/号指令》中提出“预先校验”（prior checking）要求以来，个人信息保护影响评估已成为全球普遍适用的风险管制机制。正因如此，有学者主张将匿名化过程纳入评估。〔69〕然而，考虑到《个保法》第 55 条下“对个人权益有重大影响的个人信息处理活动”的事项约束，并非所有的匿名化均需强制评估，而只有创造性使用新的匿名化技术、组织或者合并多个处理者的数据集，方符合评估的前提条件。〔70〕除上述法律适用的问题外，匿名化过程还可能由于“业务场景”的缺乏，令评估无所依托。从技术和商业逻辑观察，个人信息匿名化和匿名化信息利用是可以分离且相互独立的处理活动，是后者而非前者真正对个人信息权益造成影响。就此而言，匿名化信息的再利用才是评估的对象，由此可以理解《信息安全技术 个人信息安全影响评估指南》将“匿名化后个人信息使用场景”作为个人信息匿名化效果评估要素之一。不过，这里还有问题待解：匿名化信息既然已经不属于个人信息，能否适用个人信息保护影响评估。其实，之所以开展评估，就是出于对剩余风险的防范。换言之，评估启动就预设了匿名化可能失败，此时匿名化信息就已被假定为个人信息，评估的过程也就是检验的过程。

〔66〕 参见《日本个人信息保护法》第 37 条。

〔67〕 参见韩旭至：《大数据时代下匿名信息的法律规制》，载《大连理工大学学报（社会科学版）》2018 年第 4 期。

〔68〕 参见张新宝主编：《中华人民共和国〈个人信息保护法〉释义》，人民出版社 2021 年版，第 417 页。

〔69〕 参见赵精武：《个人信息匿名化的理论基础与制度建构》，载《中外法学》2024 年第 2 期。

〔70〕 See EPDB, *Guidelines on Data Protection Impact Assessment*, Chapter Ⅲ, B (a).

匿名信息再利用的个人信息保护影响评估制度包含了如下要素：(1) 评估时点：为了有效发现其造成的实际影响和潜在风险，评估应当在再利用处理之前进行。同时，考虑到匿名化与技术迭代、可公开获得的数据更新、法律法规变化相关，处理者应跟踪相关信息，定期开展事中评估，确保再利用风险控制在可接受水平之内。(2) 评估主体：评估由实际开展匿名化信息再利用的处理者完成。为平息可能的质疑，用户、消费者代表、业务合作伙伴、外部专家和监管机构等利益相关方均应参与其中。〔71〕在具体的程序设置上，上述参与可以融入评估的咨询环节。首先，处理者应告知处理数据的内容和属性、处理目的和方式、为实现预期目的使用的技术、系统和配置环境等，以保证利益相关方充分理解数据活动的信息。其次，在征求意见的过程中，应协助利益相关方识别风险并提出异议。最后，处理者将相关咨询反馈准确、全面、无遗漏地记录在评估报告中，这在处理者未采纳利益相关方意见和建议时尤为重要。(3) 评估适用：将匿名化信息再利用涵摄于《个保法》第 55 条之下，意味着并非所有的处理活动皆需评估，而限于法律所列出的高风险行为，特别是匿名化信息的公开和向第三方提供的场合。(4) 评估内容：与匿名化过程的评估将重心放在匿名化措施的规范性、所采用技术的通用性等问题上不同，〔72〕匿名化信息再利用的评估以个人权益为鹄的。一方面识别匿名化信息的风险来源，确定是直接使用信息造成的直接不利影响，还是作为模型输入数据造成的间接不利影响；另一方面通过“影响个人自主决定权”“引发差别性待遇”“个人名誉受损和遭受精神压力”“个人财产受损”的划分，描摹个人遭受影响的范围，最终得出影响“严重”“高”“中”“低”的定性判断。(5) 评估程序：个人信息保护影响评估不仅是识别剩余风险的措施，更是管控剩余风险的工具。为此，可采取“两阶段风险评估模式”，先初步辨识出信息利用风险，并对该风险设计出相应的风险减缓措施，继而将上述风险和减缓措施综合考量，进行第二次的评估。借此，用户可以更清楚地了解匿名化措施的风险和实效，处理者亦得以积极采取行动控制风险，最终促成各方就可接受风险的合理边界达成共识。〔73〕

五、结　语

如果说《个保法》第 1 条宣示了个人信息保护与利用的二元目标，那么匿名化条款正是落实该立法主旨的最佳工具之一。遗憾的是，徒法不足以自行。由于个人信息处理者、用户、监管机构的三重忧虑，匿名化制度在实践中窒碍难行。其实，真正的束缚来自人们的观念。对完美匿名化的追求以及对技术、法律、管理等单一措施的执念，阻止了切实可行的匿名化制度的建立。本文的研究表明，一旦从绝对安全的匿名化转向基于风险的匿名化，从彼此割裂的匿名化转到整体

〔71〕 参见刘权：《论个人信息保护影响评估——以〈个人信息保护法〉第 55、56 条为中心》，载《上海交通大学学报（哲学社会科学版）》2022 年第 5 期。

〔72〕 相关技术评估工作已体现在上文“推定匿名”的部分。

〔73〕 See NHS Digital, *Data Protection Impact Assessment-COVID-19 Vaccine Trials Permission to Contact Service-V2.0* (December 21, 2020), available at https://digital.nhs.uk/coronavirus/coronavirus-covid-19-response-information-governance-hub/data-protection-impact-assessment-covid-19-vaccine-trials-permission-to-contact-service-v1.0, last visited on Mar. 19, 2024.

系统的匿名化，匿名化条款就能起死回生，经由“推定的匿名”到“判定的匿名”再到“信任的匿名”的操作路径，为各方划定可预期的行为边界，最终实现数据价值、监管秩序和用户期待的协同共振。

Abstract：The Article 4，Paragraph 1 of Personal Information Protection Law excludes anonymized information from the category of personal information，which is known as the “anonymization clause” aimed at data circulation and utilization. However，after more than two years of implementation，the anonymization clause has hardly been used and has become a “zombie clause”，one of the biggest obstacles to the data element market. Although existing theories have fully recognized the root cause of the problem lies in the preset of zero-risk anonymization，due to the lack of precise portrayal of acceptable risks and systematic normative guidance，they are explanatory but not effective in solving the problem. By categorizing the risks of reusing anonymized information into systemic risks，operational risks，and residual risks，a concentric circle structure of “presumed anonymity” based on anonymization design，“determined anonymity” based on the interpretation of anonymization clauses，and “trusted anonymity” based on anonymization compliance has gradually formed. This not only resolves the triple concerns of personal information handlers，regulatory agencies and users，but also integrates technology and law，process and result，scenario and system，and data value and personal rights and interests. Thereby，the anonymization clause is revitalized，and a Chinese anonymization system with both operability and normativity is reborn from the ashes.

Key Words：personal information，anonymization，presumed anonymity，determined anonymity，relative anonymity

（责任编辑：王叶刚）