

数字时代个人信息合理使用的边界认定研究

吴斯

安徽财经大学法学院, 安徽, 蚌埠 233041

发布日期: 2026年6月29日

摘要

数字经济与人工智能技术的深度融合, 推动个人信息从人格权益载体向核心生产要素转型, 以知情同意为核心的传统保护模式在海量自动化处理、跨场景数据流动的数字场景中逐渐失灵, 个人信息合理使用制度成为平衡人格权益保护、数字产业发展与公共利益实现的核心制度工具。但合理使用并非无边界的免责事由, 其边界认定应以法益平衡为核心逻辑, 融合比例原则与场景完整性理论, 通过信息敏感程度、公开层级的梯度区分, 配套标准化司法权衡与技术化约束, 形成兼具规范确定性与场景适配性的认定体系, 消解保护与利用的制度张力, 为数字社会个人信息治理提供规范路径, 支撑数字经济在法治框架下高质量发展。

关键词

数字时代; 个人信息; 合理使用; 边界认定

Research on the Boundary Determination of Reasonable Use of Personal Information in the Digital Age

Si Wu

School of Law, Anhui University of Finance and Economics, Bengbu 233041, China

Abstract

With the deep integration of the digital economy and artificial intelligence, personal information has evolved from a carrier of personality rights into a core production factor. The traditional protection model centered on informed consent is increasingly incompatible with large-scale automated processing and cross-scenario data flow, making the reasonable use of personal information a pivotal mechanism for balancing personality right protection, digital industry development and public interests. Reasonable use is by no means an unrestricted exemption. Its boundary determination should take the balance of legal interests as the core logic, integrate the proportionality principle and contextual integrity theory, and build a determination system with

both normative certainty and scenario adaptability through gradient classification by information sensitivity and publicity level, coupled with standardized judicial weighing and technical constraints. This system will defuse the institutional tension between protection and utilization, provide normative support for personal information governance in digital society, and underpin the high-quality development of the digital economy under the rule of law.

Keywords

Digital Age; Personal Information; Reasonable Use; Boundary Determination

Copyright © 2026 by author(s) and Erytis Publishing Limited.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



一、绪论

数字技术的全域渗透推动人类社会进入数据驱动的发展阶段，个人信息在承载人格尊严核心价值的同时，日益成为数字经济运行、公共治理升级与科技创新突破的基础性生产要素，信息的高效流通与合理利用成为数字社会运转的核心动力。传统以知情同意为核心的个人信息保护模式，建立在工业时代单次化、场景固定的信息交换基础之上，在面对海量自动化处理、跨主体数据流转等数字时代特征时逐渐显现适配困境，同意疲劳、授权失效等问题频发，既无法为数字产业发展提供充足的制度空间，也难以实现对个人信息权益的周全保护。个人信息合理使用制度作为知情同意规则的法定例外，通过划定无需取得个人同意即可处理信息的合法范围，成为平衡人格权益、产业发展与公共利益的关键制度支点。我国《民法典》人格权编与《个人信息保护法》已搭建起合理使用制度的基本框架，明确了履行法定职责、新闻舆论监督、已公开信息处理等适用事由，但受立法技术与时代条件限制，现有规则多为原则性、开放式列举，尚未形成清晰统一、可操作的边界认定标准，导致实践中公共利益泛化解释、已公开信息滥用等问题频发，司法裁判同案异判现象突出，监管执法尺度不一，既制约了个人信息的合法有序流通，也加剧了个人信息权益受侵害的风险。围绕个人信息合理使用的边界认定，学界已从法理基础、司法适用、场景规则等维度展开诸多探讨，场景完整性理论、比例原则、动态体系论等分析工具被逐步引入本土研究，但现有成果多聚焦单一问题或单一场景，尚未形成体系化的边界认定框架，也未能实现规范缺陷、实践困境与完善路径的逻辑对应与深度契合，难以充分回应数字技术快速迭代背景下个人信息治理的复杂现实需求。对合理使用边界认定开展体系化研究，既是对人格权社会化限制理论与数据要素法治化理论的深化拓展，能够完善本土个人信息合理使用的理论体系与认定方法论。也能够为司法裁判统一权衡尺度、为市场主体明确合规边界、为监管部门细化治理标准提供规范支撑，在保障自然人人格尊严与信息权益的前提下，充分释放个人信息的要素流通价值，为数字经济高质量发展与数字社会治理现代化筑牢法治根基。

二、数字时代个人信息合理使用边界认定的现实困境

（一）法律规范供给滞后

我国现行个人信息合理使用规则散见于《民法典》第 999 条、第 1036 条与《个人信息保护法》第 13 条、第 27 条等条文，规范层面确立了法定事由加合理限度的双重结构，但在制度细化层面存在显著供给不足，形成了有制度框架、无认定标准的规范状态。从规范文本来看，立法仅对合理使用的适用事

由进行了开放式列举,包括合同履行、法定职责、紧急避险等七类情形,但对核心概念中合理的内涵与判断标准未作出明确界定,既未列明认定合理性的考量要素,也未针对不同信息类型、使用目的、公开程度设置差异化的边界规则。这种抽象化的立法模式固然保持了制度的弹性与包容性,但也直接导致边界认定的系统性不确定性。对于信息处理者而言,模糊的规则使得合规预期缺失,企业难以预判数据处理行为的合法边界,要么过度收缩数据使用范围抑制创新活力,要么肆意扩张信息使用边界侵害个人权益。对于监管机关而言,缺乏明确的认定标准导致执法自由裁量权过大,同类违法行为在不同地区、不同领域的处罚尺度差异显著,削弱了监管的权威性与统一性。对于信息主体而言,模糊的边界使得个人信息权益的范围处于不确定状态,难以有效预见自身信息的使用方式与范围,也无法及时识别并制止超出合理边界的侵权行为。

类型化标准的系统性缺失,是规范抽象化最突出的表现,也是边界认定混乱的制度根源。信息敏感程度的类型化缺失导致普通个人信息与敏感个人信息的合理使用边界不明,《个人信息保护法》虽设专章规定敏感个人信息的特殊保护规则,明确敏感个人信息处理需具备特定目的与充分必要性,但未对敏感信息的合理使用设置更严格的限制条件,导致实践中大量处理者以新闻报道、公共治理、科研统计等名义,随意采集、使用生物识别、医疗健康等敏感信息,弱化了敏感信息的特殊保护强度,使得人格尊严的核心防线面临失守风险。使用目的的类型化缺失导致公益目的与商业目的的差异化边界不清,法定合理使用事由中既包含纯粹的公共利益目的,也包含兼具公益属性与商业属性的行为,甚至部分事由可被商业主体随意包装利用,例如企业将爬取公开信息优化产品、训练人工智能模型等商业行为包装为科研统计,进而主张合理使用豁免。立法未对不同性质的目的设置梯度化的认定标准,使得商业利益常借公益之名扩张边界,架空了合理使用制度的公益属性初衷。信息公开程度的类型化缺失导致未对已公开信息进行分层界定。《个人信息保护法》第27条仅笼统规定可在合理范围内处理已公开信息,但未区分绝对公开信息与相对公开信息的不同保护层级。政务公示等面向全社会主动公开的信息,信息主体的隐私期待较弱,合理使用的范围可适度放宽,而社交平台、短视频平台等用户在特定圈层内公开的个人信息,信息主体仍保有较强的隐私期待与场景预期,合理使用的范围理应受到严格限制。规范层面的类型化空白,直接导致实践中对已公开信息的合理使用边界认定混乱,爬虫抓取社交平台个人信息用于商业用途的行为屡禁不止,司法裁判也难以形成统一判断。

（二）司法裁判尺度不一

法定规范的抽象化最终传导至司法层面,表现为个人信息合理使用边界认定的裁判尺度不一、同案异判现象突出,其本质是司法裁判缺乏统一的权衡方法与论证框架,法官的自由裁量缺乏有效约束。当前司法实践中,针对个人信息合理使用的抗辩审查普遍存在重事由、轻限度的倾向,多数裁判仅对被诉行为是否落入法定事由范畴进行形式审查,只要行为大致符合新闻报道、公共利益、已公开信息等事由外观,便直接认定构成合理使用,而对行为是否超出合理限度缺乏实质性审查,导致合理使用的边界被不当放宽。这种审查模式的核心缺陷,在于未建立起体系化的利益权衡方法,比例原则与场景完整性理论等核心分析工具未得到普遍、规范的适用。一方面,比例原则的适用流于形式,多数判决仅对行为的目的正当性进行判断,即确认行为是否服务于公共利益或法定事由,而未对手段的必要性与法益的均衡性进行实质审查。例如在公共场所人脸识别纠纷中,部分法院仅以维护小区安全具备正当目的为由,认定物业采集人脸信息属于合理使用,却未审查是否存在门禁卡、密码等侵害更小的替代方案,也未权衡业主的人格权益与物业管理效率之间的轻重关系,使得比例原则沦为纯粹的正当性背书,无法发挥限制边界的作用。另一方面,场景完整性理论的适用缺位,多数裁判未将信息的初始披露场景作为边界认定的考量因素,忽视了信息主体对信息使用的场景预期。个人信息的公开具有场景依赖性,自然人在特定

场景下披露个人信息，并不意味着同意在其他无关场景下被使用，例如用户在求职平台公开简历信息，是为了获得就业机会，而非同意企业将其信息用于商业营销或人工智能模型训练。但当前司法实践中，大量判决仅以信息已公开为由直接认定合理使用，完全不考量后续使用场景与初始披露场景是否一致，导致信息主体的场景预期落空，个人信息的自决权被架空。

损害认定标准的偏差与举证责任的失衡，进一步加剧了司法边界认定的混乱。在损害认定层面，传统侵权法以实质损害为核心，要求原告证明存在明确的财产损失或精神损害，但数字时代个人信息侵害具有隐蔽性、累积性特征，很多超出合理边界的信息处理行为，虽未造成直接的现实损害，却会带来隐私泄露、算法歧视等潜在风险，对个人的人格利益造成隐性侵害。当前多数法院仍固守传统的实质损害标准，以未发生实际损害为由否定侵权成立，使得大量超出合理边界的信息处理行为无法得到司法规制，合理使用的边界被持续稀释。在举证责任分配层面，现行规则遵循谁主张、谁举证的一般原则，由原告证明信息处理行为超出合理使用边界，但个人信息处理的全流程掌握在处理者手中，算法的运行逻辑、数据的流转路径、信息的使用范围均处于不透明状态，信息主体难以获取相关证据，根本无法完成举证责任。而信息处理者只需提出合理使用的抗辩，无需对行为的合理性承担举证责任，这种举证责任的不对等，使得合理使用抗辩极易成为信息处理者规避侵权责任的工具，司法难以发挥矫正边界、救济权利的作用。

（三）规则适用边界不清

数字技术的快速迭代持续催生新型个人信息处理场景，生成式人工智能等技术的广泛应用，突破了传统合理使用制度预设的适用场景与行为模式，使得原本就模糊的边界认定面临更大的失控风险。现行立法制定时，主要针对传统的线下与浅度互联网信息处理模式，未充分预见数字新技术对合理使用边界的系统性冲击，导致新兴场景下规则供给严重不足，形成大量规制真空。生成式人工智能的爆发式发展，使得训练数据的合规性成为个人信息合理使用的核心争议领域。大模型训练需要海量的数据素材，其中大量来源于网络公开的自然人肖像、声纹等个人信息，训练数据提供者普遍主张网络公开信息属于已公开个人信息，抓取用于模型训练属于合理使用范畴。但这种主张忽视了训练对传统边界的突破。传统的已公开信息合理使用多为少量、有限的使用，而人工智能训练是对全网公开信息的批量、无差别抓取，使用规模与范围远超立法预设的合理尺度。同时，人工智能训练并非对信息的直接使用，而是通过算法提取特征后生成新的内容，后续生成服务往往具有明确的商业属性，属于典型的衍生商业使用，与传统科研统计的公益属性存在本质区别。人工智能模型具备强大的再识别能力，即便训练数据经过初步去标识化，也可能通过模型运算重新识别到特定自然人，使得匿名化的保护屏障失效，信息主体面临的人格权益风险被无限放大。现行规范仅笼统要求人工智能训练数据来源合法，并未明确公开信息用于训练的合理使用边界，也未针对敏感信息、衍生商业使用设置特殊限制，个人信息权益面临大规模侵害的风险。

自动化决策与生物识别技术的普及，也从不同维度消解着合理使用的传统边界。自动化决策与用户画像技术的广泛应用，使得平台得以基于收集到的用户信息构建精细化的用户标签体系，开展精准营销、个性化推荐甚至大数据杀熟，却常以优化服务为由主张合理使用，规避用户的同意义务。自动化决策本质上是对个人信息的深度分析与商业化利用，并非纯粹的科研统计行为，其直接服务于平台的商业利益，且会对用户的交易公平、自主选择产生实质影响，但现行规则未明确区分科研统计与商业画像的边界，使得平台得以借科研之名行商业利用之实，不断扩张个人信息的使用边界。此外，公共场所生物识别技术的广泛部署，也使得公共利益与个人权益的边界持续模糊。人脸信息属于核心敏感个人信息，其采集与使用本应受到最严格的限制，但当前大量商场、景区等场所无差别安装人脸识别设备，强制采集消费者的人脸信息，并普遍以公共管理为由主张合理使用，导致实践中人脸采集的边界持续扩张，敏感个人

信息的保护防线不断被突破。

三、数字时代个人信息合理使用边界认定的完善路径

（一）细化法律规范体系

针对法定规范抽象化、类型化缺失的问题，应当在现行法律框架基础上，通过行政法规、司法解释等层级的规范细化，构建信息分层和公开分级”的类型化边界认定标准，将抽象的合理概念转化为可操作的法定规则，从规范源头明确合理使用的边界。应当在规范层面确立合理使用的双重边界结构，明确合理使用的成立不仅需要满足法定事由的合法性要求，还必须符合合理限度的实质性标准，并将目的正当性、手段必要性、场景匹配性、损害可控性四项要素确立为认定合理限度的法定考量要素，为司法裁判与监管执法提供统一的规范依据。在此基础上，针对不同维度推进类型化规则细化，构建梯度化的边界标准。其一，按信息敏感程度分层，设置差异化的合理使用门槛。普通个人信息适用一般合理性标准，而敏感个人信息由于承载着核心人格利益，应当适用严格限制的合理使用规则。明确敏感个人信息的合理使用仅适用于重大公共卫生事件、司法机关办案、未成年人保护等核心公共利益场景，纯粹商业目的、一般公共管理场景一律不得适用敏感信息的合理使用。即便在法定公益场景下使用敏感信息，也必须满足强制去标识化、专人权限管理等严格条件，缺少任一条件即认定超出合理边界，从规范层面强化敏感信息的保护强度。其二，按使用目的的性质分阶，划定不同的合理使用范围。将合理使用的目的划分为纯粹公益目的与衍生商业目的两个层级，对于纯粹的公共利益目的，合理使用的范围可适度放宽，只要满足四项基本要素即可适用豁免。对于衍生商业目的，即便其过程包含科研统计等环节，也应当严格限缩合理使用的适用范围，明确仅能使用完全匿名化、无法复原身份的信息，可识别的个人信息不得适用合理使用豁免，必须取得信息主体的单独同意，防止商业利益借公益之名侵蚀个人权益。其三，按信息的公开程度分级，明确已公开信息的差异化边界。将已公开个人信息划分为绝对公开信息与相对公开信息，绝对公开信息指国家机关依法公示、信息主体主动向全社会公开的信息，此类信息的隐私期待最弱，合理使用的范围可适度放宽，允许合法爬虫抓取用于公共治理、科研统计等场景，但仍不得用于精准画像、深度合成等侵害个人重大利益的用途。相对公开信息指用户在特定平台场景下公开的信息，此类信息信息主体仍保有较强的隐私期待与场景预期，除新闻舆论监督、法定公共利益等特殊情形外，商业使用一律不得主张合理使用，必须取得信息主体的单独同意，从规范层面纠正凡公开即可随意使用的错误认知。

（二）统一司法裁判框架

以法定四要素为基础，构建统一的动态权衡裁判方法，同时完善举证责任、损害认定、类案指引等配套规则，规范法官自由裁量权的行使，实现同案同判。首先，应当确立合理使用抗辩的举证责任倒置规则。基于信息处理者与信息主体之间的技术能力与信息不对称地位，明确当信息处理者主张其行为构成合理使用时，应当由处理者承担举证责任，证明其行为符合全部四项要件，而信息主体仅需证明处理者实施了针对其个人信息的处理行为，无需证明行为超出合理边界。通过举证责任倒置，既可以降低信息主体的维权门槛，也能够倒逼处理者规范自身的数据处理行为，留存完整的合规记录。其次，构建标准化的裁判方法，明确每个要素的审查标准与论证要求，规范法官的自由裁量过程。法官在裁判过程中，应当对四项要素逐一进行审查论证，形成完整的权衡逻辑，禁止仅以信息已公开、目的正当等单一理由直接认定合理使用，强化裁判说理的规范性与严谨性。此外，还应当通过发布指导性案例、类案裁判指引等方式，统一高频案件的裁判尺度。最高人民法院可针对网络爬虫、生成式人工智能、自动化决策等合理使用纠纷高发的场景，发布专门的指导性案例与类案审理指南，提炼统一的裁判规则与认定标准，为各级法院审理同类案件提供明确指引，减少同案异判现象。同时，完善合理使用侵权的损害赔偿标准，

根据侵权行为的性质、范围、后果设置梯度化的赔偿规则。对于轻微超出合理范围、未造成实质损害的，判令停止侵害、删除信息。对于批量抓取、大规模侵害众多个人信息权益的，适用惩罚性赔偿，提高侵权成本。对于侵害敏感个人信息、造成严重精神损害的，大幅提高精神损害赔偿数额，强化司法裁判的震慑作用。

（三）构建规则适用边界

针对数字新技术带来的边界冲击与规则空白，应当立足不同技术场景的运行特征，制定专门的边界认定规则，同时推动法律规则与技术治理深度融合，以技术手段固化合理使用的边界，实现法律与技术的协同治理。针对生成式人工智能训练数据的合规问题，应当明确人工智能训练场景下个人信息合理使用的边界规则，区分训练阶段与生成应用阶段设置差异化要求。在训练阶段，处理者抓取网络公开信息用于模型训练的，若仅涉及普通个人信息，且训练目的为非营利性科研，则可适用合理使用，但必须满足严格的合规要求，一是必须对数据进行去标识化处理，采取差分隐私等技术措施确保数据无法被重新识别到特定自然人。二是训练数据的抓取与使用不得违反信息主体的明确拒绝声明，不得抓取信息主体设置了访问权限的非公开信息。三是训练过程中不得对个人信息进行二次流转共享，仅限用于模型训练。若训练涉及肖像、声纹等敏感个人信息或训练模型用于商业化服务，则不得适用合理使用豁免，必须取得信息主体的单独同意或使用获得授权的合规数据集。在生成应用阶段，模型生成内容涉及特定自然人的个人信息的，必须符合合理使用的法定事由，不得利用深度合成技术侵害他人人格权益，服务提供者应当对生成内容的合规性承担审核责任。

针对自动化决策与生物识别两类高频争议场景，应当进一步明确边界规则，针对自动化决策与用户画像场景，应当明确科研统计与商业利用的边界，严格限定科研统计类合理使用的适用范围。明确只有纯粹非营利性的学术研究等行为才可主张科研统计类合理使用，且必须使用匿名化的聚合数据，不得针对特定个人进行画像分析。互联网平台基于用户信息构建用户画像、开展精准营销等商业行为，不属于合理使用的范畴，必须取得用户的同意，并赋予用户拒绝自动化决策的权利。平台不得以优化服务、提升体验等为由，变相规避用户的同意义务，不得将用户同意作为使用服务的强制条件。针对公共场所生物识别场景，应当严格限定公共安全的适用范围，明确只有公安机关、国家安全机关等法定机关基于维护公共安全的法定职责，才可适用合理使用采集人脸等生物识别信息。监管部门应当加大对公共场所违规人脸采集的整治力度，明确违规采集的认定标准与处罚尺度，守住敏感个人信息的保护底线。在此基础上，应当建立技术合规的强制标准，推动法律边界的技术化落地，要求信息处理者在数据系统中内置边界控制机制，将合理使用的法律要求转化为技术系统的硬性约束。通过技术手段将法律边界固化为系统不可突破的约束，从技术源头减少超出合理边界的信息处理行为，实现法律规则与技术治理的良性互动。

四、结语

个人信息合理使用边界的法治化建构，本质上是数字法治进程中人格尊严保障与数据要素价值释放的价值调和与制度平衡，其制度意义不仅是对个案中权利义务的厘清，更关乎整个数字社会的信任根基与治理底色。在数字中国建设与数据要素市场化改革的宏观背景下，清晰稳定、可预期的合理使用边界既是守护自然人人格主体性、避免个体在算法与数据洪流中被客体化的法治防线，也是降低数字产业合规成本、激活数据要素流通潜能、培育公平有序数字市场生态的制度基石。真正成熟的数字治理是通过精细化的规则设计与体系化的治理机制，让技术创新始终运行在人文关怀的制度轨道之上，让数据流通始终恪守权利保障的法治底线。面向未来，随着生成式人工智能、物联网等技术的持续演进，个人信息的处理场景将不断拓展，边界认定的规则也需始终保持与技术变革的同频适配，在动态调适的过程中不

断趋近数字正义, 最终实现人的全面发展与数字社会高质量发展的协同统一。

参考文献

- [1] 柴炳. 合理使用场景下个人信息权益实现的限度[J]. 社会科学战线, 2026, (6): 272-280.
- [2] 吴沛山. 非法使用公民个人信息行为的规制路径[J]. 江苏社会科学, 2026, (1): 196-205.
- [3] 屈然, 张健文. 肖像合理使用规范冲突和疏漏的消解[J]. 当代法学, 2025, 39 (3): 58-69.
- [4] 娄秉文. 数字人权视阈下个人生物识别信息合理使用制度构造[J]. 江苏大学学报(社会科学版), 2025, 27 (2): 83-93.
- [5] 屈然. 私密信息商业化利用的证立及制度建构[J]. 学海, 2024, (6): 184-194.
- [6] 张涛. 生成式人工智能训练数据集的法律风险与包容审慎规制[J]. 比较法研究, 2024, (4): 86-103.
- [7] 赵桐. 双重法益构造下的个人信息圈层式刑法保护[J]. 东南大学学报(哲学社会科学版), 2024, 26 (4): 87-97.
- [8] 胡宏涛. 论生成式人工智能服务提供者的个人信息合理使用[J]. 江苏社会科学, 2024, (2): 185-192.
- [9] 尹建国, 周采擎. 论政府数据开放中的个人信息合理使用[J]. 山西大学学报(哲学社会科学版), 2024, 47 (2): 38-48.
- [10] 王东方. 生成式人工智能对个人信息权益的侵害风险及其法律规制[J]. 征信, 2024, 42 (2): 31-37.
- [11] 杨芳. 重构公开个人信息处理的特殊合法事由——以区分自行公开与他人合法公开为核心[J]. 比较法研究, 2023, (6): 154-169.
- [12] 吴晓丹. 私密信息合理使用的规范体系及其限制[J]. 华东政法大学学报, 2023, 26 (5): 56-69.
- [13] 王冉冉. 已公开的个人信息的合理使用及其缩限[J]. 现代法学, 2023, 45 (4): 46-58.
- [14] 吴国喆, 王文文. 数据共享视域下个人信息“合理使用”的场景化判定[J]. 西安交通大学学报(社会科学版), 2023, 43 (3): 142-156.
- [15] 刘磊. 论私密个人信息的合理使用困境与出路[J]. 财经法学, 2023, (2): 36-50.
- [16] 刁胜先, 刘韵. 数字经济时代个人信息合理处理制度研究[J]. 科技与法律(中英文), 2022, (6): 11-21.
- [17] 卢勤忠, 张宜培. 非法使用个人信息行为入刑的立法构思[J]. 河北法学, 2023, 41 (1): 73-96.
- [18] 张涛. 生成式人工智能训练数据集的法律风险与包容审慎规制[J]. 比较法研究, 2024, (4): 86-103.