财经法学 No. 5，2024
pp. 41 - 58

个人信息匿名化制度的反思与改进

夏庆锋*

内容提要：我国《个人信息保护法》第73条规定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，并在第4条对匿名化信息进行豁免保护，采用静态匿名化的方法平衡个人信息保护与个人信息利用。但是，伴随社会信息化以及网络技术的快速发展，匿名化信息与非匿名化个人信息的界限趋于模糊，强大的经济激励使去匿名化具有针对性，导致重新识别的匿名化信息对信息主体产生侵害风险甚至现实损害。虽然已有网络服务商承诺、合同义务约定与立法直接禁止等措施对去匿名化进行制约，但未能实现较好的规制效果，应在现有匿名化制度中加入更为灵活的动态匿名化方法。当匿名化信息的使用可能产生损害或是由于语境的变化使匿名化信息具有识别性时需进行更为严格的再匿名化处理，否则不真正匿名化信息仍需受到法律保护。

关键词：个人信息　匿名化信息　去匿名化　动态匿名化　比例原则

《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）对个人信息进行定义，其第4条第1款规定“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”。在个人信息收集、使用等处理过程中，基于保护个人信息与最大化利用个人信息的平衡考虑，匿名化措施得以提出。所谓匿名化，指从收集的个人信息中删除可识别信息，使对该信息的使用、分析、研究等活动无法追溯至信息主体。立法上对匿名化信息多进行豁免处理，例如我国《个人信息保护法》第4条第1款后半句规定“不包括匿名化处理后的信息”。欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）序言第26条规定：“数据保护原则不适用于匿名信息，即与已识别或可识别自然人无关的信息，亦不适用于能够使得数据主

* 夏庆锋，安徽大学法学院副教授、安徽网络法治研究中心研究人员。

本文为2023年度安徽省高等学校科学研究重大项目“网络空间合同格式条款的效力研究”（2023AH040005）的阶段性成果。

体不可识别或不再可识别的匿名化个人数据。因此本条例亦不适用于对类似匿名信息的处理，包括基于数据统计或研究目的。”〔1〕美国联邦贸易委员会（Federal Trade Commission，FTC）也认为数据不具有合理可链接性时应被排除在数据保护框架之外。〔2〕未将匿名化信息纳入法律保护范畴有利于促进信息的自由流动，尤其体现在网络空间提升产品质量与提高服务水平等活动中。然而，实践中去匿名化具有的可操作性与巨大经济利益导致匿名化无法不可逆转地保护信息主体，如伴随相关技术的不断发展，信息中介能够将匿名化信息与辅助信息相结合从而重新识别对应的自然人主体，进而造成侵害。我国立法采用静态匿名化方法，即明确规定匿名化信息的概念和特征，认定个人信息被匿名化后无法链接至信息主体，并为匿名化信息的处理行为提供“安全的避风港”，导致个人信息主体受到去匿名化行为侵害风险或实际损害时无法得到法律保障或进行救济。虽然可将去匿名化的个人信息重新纳入《个人信息保护法》的保护范畴，但考虑到程序上的复杂性以及实际操作过程中个人信息主体处于被动依赖的劣势地位，去匿名化的隐蔽过程无法被及时发现，且即使发现个人信息受到侵害也难以进行因果关系举证。因此，为了在保证个人信息安全的同时促进其效用价值的发挥，应当提升匿名化措施后的信息不被去匿名化的水平，并在发现存在去匿名化风险时及时进行再匿名化处理。

一、匿名化信息及适用标准

隐私法与个人信息保护法对个人信息的保护规定限制其完全自由流动，例如《中华人民共和国民法典》（以下简称《民法典》）第 1034 条规定“自然人的个人信息受法律保护”以及第 1035 条规定处理个人信息应当“征得该自然人或者其监护人同意”，又如我国《个人信息保护法》第 13 条规定个人信息处理者需要符合七种情形方可处理个人信息，而信息的自由流动对于科学研究、现象分析以及其他重要政治和经济职能的发挥具有关键作用。艾拉·鲁宾斯坦和伍德罗·哈佐格认为：“对信息收集和披露的全面和强有力的禁令将会对组织和整个社会造成不可思议的代价，即使这样的限制是明智的与政治上可接受的，关闭个人信息的研究和流动性将是毁灭性的”。〔3〕适用匿名化信息有利于对个人信息进行保护并促进个人信息流动，使有价值但敏感的个人信息得以发布，并减少这些信息与信息主体的关联，被誉为“两全其美的妥协”。

（一）个人信息的匿名化

现代社会存在各种各样的匿名化技术，包括抑制、泛化、聚合、添加噪声、替代等，使对匿名化信息的使用满足个人信息保护法律的豁免要求，这些技术在不同程度上平衡个人信息保护与

〔1〕 中国信息通信研究院互联网法律研究中心、京东法律研究院编：《欧盟数据保护法规汇编》，中国法制出版社 2019 年版，第 17 页。

〔2〕 See Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*, available at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, last visited on Jul. 21, 2023.

〔3〕 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 731 (2016).

个人信息利用。〔4〕“抑制”指从个人信息集中完全移除可识别信息，虽然这种技术为信息主体提供最稳妥的保护，但同时也大大降低匿名化信息的效用。“泛化”仅涉及修改标识符，例如显示一个人的出生时间而不是完整的日期，这种技术的优势在于妥善顾及个人信息的效用性，但对于信息主体提供的保护效力较弱。保罗·欧姆将“抑制”与“泛化”视为“发布即遗忘技术”，一旦个人信息管理员修改信息并发布记录，其将遗忘匿名化信息，不仅不会跟踪发布后数据的变化，也很难甚至无法撤回已发布内容。〔5〕聚合、添加噪声与替代技术通过阻碍对原始信息的查看大大降低匿名化信息与信息主体的可链接性，“聚合”通过对共享某些个人信息元素的信息主体进行分组来提供概括性信息，“添加噪声”将不精确的信息或数据插入原始信息集中，“替代”则是利用其他参数直接替换原始信息。〔6〕

我国《个人信息保护法》对匿名化与相近概念进行区分，例如第73条规定匿名化“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”，去标识化“是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程”，立法上认为匿名化指不可逆过程，而去标识化具有可逆性。本文认为需进一步思考两者之间的界限。匿名化与去标识化过程都是去除个人信息中具有可识别性的内容，只是匿名化需删除或加密所有具有可识别性的内容，而去标识化可以仅仅去除姓名、身份证号码等直接标识符或同时去除可将个体区分开而又不能直接识别个体的网络和设备ID等间接标识符，两者本质上都是去除可识别性内容，只是程度上存在差异，而不存在十分清楚的界限。〔7〕美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）发布的《保护个人可识别信息机密性的指南》（Guide to Protecting the Confidentiality of Personally Identifiable Information）规定去识别信息为“删除或隐藏足够多的个人可识别信息的记录，使得剩余信息无法识别信息主体身份，并且没有合理依据相信该信息可用于识别信息主体”，该规定包含对匿名化与去标识化的定义，并没有刻意区分。〔8〕我国《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第9.2（b）条规定“向个人信息主体告知共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果，并事先征得个人信息主体的授权同意。共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的除外”，该规定表达出处理个人信息应事先征得个人信息主体的同意，但是若共享、转让“去标识化处理的个人信息”则无需获得同意，该去标识化处理的个人信息应达到“数据接收方无法重新识别或者关联个人信息主体”的标准。所谓数据接收方无法重新识别或关联个人信息主体，实质上体现匿名化信息的内在含义，前述规定反映出去标识化信息与匿名化信息的

〔4〕 参见刘湘雯、王良民：《数据发布匿名技术进展》，载《江苏大学学报（自然科学版）》2016年第5期。

〔5〕 See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1712 (2010).

〔6〕 See Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 758 - 759 (2016).

〔7〕 欧美在相关制度上也具有共同性，例如欧盟使用“匿名化”和“假名化”制度，美国使用“去身份化”制度，这三种制度并没有本质区别。参见刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020年第12期。

〔8〕 See National Institute of Standards and Technology, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, available at http://csrc.nist.gov/publications/nistpubs/800 - 122/sp800 - 122.pdf, last visited on Feb. 2, 2024.

概念混同性。网络服务商处理活动中也没有对匿名化与去标识化进行区别规定，例如《微博个人信息保护政策》第三项“我们如何委托处理、共享、转让及公开披露您的个人信息”中第 2.3 条规定：“为实现程序化广告推送，我们可能会与广告合作伙伴（包括广告主和其他广告服务提供商）共享去标识化或匿名化处理后的信息，以帮助其在不识别您个人身份的前提下提升广告的有效触达率。”〔9〕该规定并未对去标识化信息或匿名化信息进行区分，而是统一认定为不识别个人身份前提下扩大广告效果的有力措施。

（二）匿名化信息的适用标准

互联网经济的发展使大量信息充斥在网络空间，法律不可能监管所有的信息流动，如果没有清晰的监管边界，个人信息及隐私权益的法律保护就会扩大到几乎无限的信息内容，最终导致整个社会的经济发展停滞甚至瘫痪。〔10〕因此，在法律层面确立匿名化信息的定义并按照一定标准进行适用有利于明确信息监管的边界，使得隐私法与个人信息保护法只规制具有可识别性的个人信息而豁免匿名化信息，从而发挥信息的效用价值。匿名化信息的适用标准应当强调信息被匿名后的不可链接性。例如，欧盟第 29 条数据保护工作组发布意见对欧盟 1995 年《数据保护指令》（Data Protection Directive，DPD）第 26 条“豁免匿名化数据不受任何监管”的法律规定进行评价，强调“一个重要因素是匿名化处理必须不可逆转”，以及“像删除一样永久，即不可能重新识别个人数据”〔11〕。第 29 条数据保护工作组认为，匿名化技术可以提供隐私保护，并可能被用于生成高效的匿名化结果，但前提是应用程序设计得当。因此需要根据具体情况以及不同技术组合，明确何种匿名化信息符合豁免要求，构建匿名化信息的适用标准。个人信息处理者或者其他主体通过匿名化个人信息对信息主体的各项权益进行保护，不同场景对可识别信息的要求不同，有的只需删除直接标识符，有的则需同时删除直接标识符与间接标识符，从而防止对信息主体的隐私侵害或个人信息非法利用。

匿名化信息的适用标准应至少包含三层维度，分别对相同组织的其他成员、特定第三方与公众群体等接收主体适用不同的标准。相同组织的其他成员与匿名化处理主体具有紧密联系，但基于个人信息保护的考虑仍需进行匿名化。例如，医院收集并处理病人信息后向其附属的科研部门提供匿名化信息以供科学研究与难题攻关，此时的匿名化程度较低，只需对个人的姓名、联系电话等直接标识符进行删除或隐藏即可，以便于科研部门对目标数据进行病理特征或发展趋势的研究，否则将影响对信息的利用效率。特定第三方涉及网络服务商与通过分析个人信息提升产品与服务质量的广告商等其他信息中介，其利用个人信息对用户进行精准营销进而侵害个人生活安宁与人格自由发展等基本人格权益，因此需要进行完整的匿名化操作，此时的匿名化程度较高。例如，门户网站收集用户个人信息并进行匿名化处理后向第三方广告商提供，广告商在获取匿名化信息后基于更大盈利的考虑往往会试图找出目标用户的详细个人信息。为了防止广告商进行违法

〔9〕《微博个人信息保护政策》，载 https://www.weibo.com/signup/v5/privacy，最后访问时间：2023 年 8 月 11 日。

〔10〕参见程啸：《论个人信息权益与隐私权的关系》，载《当代法学》2022 年第 4 期。

〔11〕Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, last visited on Jun. 11, 2023.

操作进而损害信息主体权益，应当进行更为严格的匿名化处理，除了删除直接标识符外，还需删除不具有直接识别性的间接标识符。第三类接收主体为普通公众，例如研究机构对大量志愿者的个人信息进行收集、分析，得出结论后再向公众发布，此时当然需要进行匿名化处理，但是与向特定第三方提供的匿名化信息不同，向公众群体提供的匿名化信息一般为大的趋势或具有高度概括性的结论，不含有涉及个人的任何标识，此时的匿名化程度最高。〔12〕

二、匿名化信息具有去匿名化风险

匿名化信息的定义具有挑战性，如果其定义过窄，则太多的信息流动将受到个人信息保护法的规制，进而使得个人信息保护法成为一种对几乎所有信息进行繁琐规定的监管制度，而定义过宽则造成太多个人信息不被法律保护，使个人信息保护法变得无关紧要。尤其在数据挖掘和行为营销等现代技术的背景下，伴随个人信息收集与分析技术的进步而产生的去匿名化措施使个人信息与匿名化信息之间的界限逐渐模糊。〔13〕去匿名化是匿名化的逆措施，指对于已经删除标识符的个人信息进行重新识别并找到信息主体的过程，该措施的出现与快速发展使匿名化信息接收者能够进行重新识别。匿名化信息具有去匿名化风险，试图重新识别个人信息的实体可以利用辅助信息找到匿名化信息背后的自然人，再将该自然人链接到匿名化信息中，从而进行去匿名化处理。多数个人信息保护法与数据保护法在立法时去匿名化技术并不成熟，彼时对已经匿名化的信息进行重新识别不具有可行性，因此，我国《个人信息保护法》与欧盟《通用数据保护条例》等个人信息综合性法律，以及美国《格雷姆-里奇-比利雷法案》（Gramm-Leach-Bliley Act，GLBA）与美国《健康保险携带和责任法案》（Health Insurance Portability and Accountability Act，HIPAA）等专门性法律皆对匿名化信息与非匿名化个人信息进行二分法处理。〔14〕但是，网络技术的快速发展以及强大的经济激励使得去匿名化具有可行性与针对性，导致对非匿名化的个人信息进行保护而对匿名化信息进行豁免处理的匿名化制度存在弊端，尤其在匿名化信息被重新识别后丧失法律保障或无法进行及时的法律救济。绝对意义上“匿名化信息不能重新识别”的静态标准过于理想化，而这种理想化来源于对匿名化技术的绝对信心，从而导致制度安排上的不周全。〔15〕

（一）技术进步使去匿名化具有可行性

技术进步使具有正确外部信息的信息中介能够利用匿名化信息的剩余效用揭示已经匿名化的各项信息，例如智能设备及其所具有的算法系统可以主动收集各项匿名化信息并与正确的辅助信息进行配对、互联网 Cookie 程序能够追踪匿名用户的网络行为从而精确识别具体个人等。因此，

〔12〕 参见〔美〕克莱·舍基：《人人时代：无组织的组织力量》，胡泳、沈满琳译，浙江人民出版社 2015 年版，第 8－12 页。

〔13〕 参见王立梅：《大数据视角下的个人信息匿名化规则构建》，载《云南民族大学学报（哲学社会科学版）》2021 年第 5 期。

〔14〕 美国《格雷姆-里奇-比利雷法案》要求金融机构向消费者提供不将其非公开的个人信息共享给第三方的选择机会，但同时也规定如果信息“不包含账号、姓名或地址等个人标识符的汇总信息或盲数据”，则不应被视为个人身份信息，也不受该法规的监管。See 16 C. F. R. § 313. 3 (o) (2) (ii) (B) (2008). 美国《健康保险携带和责任法案》隐私规则明确豁免去识别健康信息，“允许使用重要信息的同时保护寻求治疗的人的隐私”。See 45 C. F. R. § 164. 502 (d) (2) (2017).

〔15〕 参见姚佳：《个人信息主体的权利体系——基于数字时代个体权利的多维观察》，载《华东政法大学学报》2022 年第 2 期。

至少对于有用的信息集与数据库而言，完美的匿名化难以实现，总有一些外部信息可以与匿名化信息结合，从而揭示个人真实信息。

1. 智能设备自动识别个人信息

为了提高产品与服务质量，商家在生产智能设备时添加信息收集功能，即使用户采取匿名的方式使用，该种设备也将尽可能多地收集信息以便对信息主体进行识别，进而提供更加符合用户需求的服务。例如，物联网的发展越来越多地将日常物品连接至网络，包括家庭自动化系统、自动驾驶汽车、汽车跟踪设备和智能医疗设备等，这些设备通过收集用户信息进行功能优化，同时也为商家收集个人信息创造新的渠道。智能设备能够直接收集敏感信息，例如精确的地理位置、金融账户或健康信息等。〔16〕而且，伴随智能设备的使用种类和范围不断扩大，即使未能直接收集用户敏感信息，其也可以通过对大量匿名化信息的去匿名化操作推断出正确的个人信息。

对于智能设备而言，删除姓名、电话号码、地址、单位等具有识别符的信息内容并不能阻碍去匿名化过程，因为“剩余的数据仍然可以帮助商家重新识别用户，方法是将数据链接或匹配到其他数据库，或查看数据库字段和记录本身的独特特征”〔17〕。该方法也被称为“信息累积方法”，指一旦信息收集者将两个或多个信息集结合在一起，则可以将新链接的匿名化信息添加到已识别的其他信息中，并使用这些信息帮助解锁匿名化信息。阿尔温德·纳拉亚南和维塔利·施玛蒂科夫提出：“一旦任何数据与一个人的真实身份相关联，该数据与其他任何数据的关联都会破坏后者的匿名性。”〔18〕例如，用户在购买智能设备时只提供常用的电子邮箱地址，由于智能设备具有网络连接性，当其在网络空间搜索到用户使用电子邮箱地址的其他行为和匹配信息时，将自动收集并发回生产商家，以便商家对用户信息进行累积收集并重新识别更多匿名化信息。因此，甚至只是暴露非敏感个人信息的重新识别事件也具有极大侵害风险，原因在于它们增加特定信息的可链接性，从而使信息主体在未来承受更多个人信息泄露和侵害风险。正如欧姆所述，一旦数据收集者能够将一个匿名化数据与数据主体同步，则他们还能够将合并后的个人数据与第二个匿名化数据进行匹配，然后是第三个，以此类推直至建立完整的个人数据库。〔19〕

2. IP 地址确认与 Cookie 软件跟踪

用户使用网络服务通过不注册网站账号或要求网络服务商不跟踪等形式进行匿名化操作，但这种“匿名化操作”具有迷惑性。由于 IP 地址是宽带连接所必须配备的且不会改变，一旦计算机连接至互联网，就已经产生一个基本的内置识别系统。〔20〕网络服务商可以通过固定的 IP 地址获得用户“数据指纹”，使基于删除个人可识别信息以对匿名化信息进行豁免使用的立法意图变

〔16〕 参见朱晓峰、黎泓玥：《私密信息与敏感个人信息区分保护论》，载《经贸法律评论》2023 年第 1 期。

〔17〕 Latanya Sweeney, *Maintaining Patient Confidentiality When Sharing Medical Data Requires a Symbiotic Relationship Between Technology and Policy 6*, available at http://privacy.cs.cmu.edu/dataprivacy/projects/law/aiwp.pdf, last visited on Apr. 13, 2023.

〔18〕 Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, available at http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, last visited on Sep. 18, 2023.

〔19〕 See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1725 - 1727 (2010).

〔20〕 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。

得徒劳，“对于拥有外部信息权的主体而言，一切信息都是个人可识别信息”〔21〕。

Cookie 软件也是对匿名化信息进行去匿名化处理的有效工具，网络服务商能够利用 Cookie 对用户进行跟踪分析，使得匿名状态下的网络行为可以精准追踪到具体个人。美国联邦贸易委员会解释道：“这种对消费者来说通常是无形的做法，允许企业将他们的广告更紧密地与推断的受众兴趣联系在一起。企业通常使用‘Cookie’来跟踪消费者的在线活动，并将这些活动与特定的电脑或设备联系起来。”〔22〕从 20 世纪 90 年代起，Cookie 被用于在不同网页之间传递信息，并对重复访问者进行重新识别。〔23〕由于早期浏览器设立的安全策略，Cookie 存储的信息并不能被其他网站访问，只允许特定网站在特定范围内跟踪用户的网络行为，因此起初被称为“第一方 Cookie”的技术并不会造成太大的隐私问题。〔24〕但是，随着网络技术的发展，Cookie 已经衍变为信息共享技术并在网站中无处不在。例如，跨域跟踪即通过第三方放置在不同网站上的 Cookie 予以实现，网络服务商通常在用户的计算机上放置一个 Cookie 软件并根据用户访问的网站范围创建用户配置文件，当用户从一个网站转移至另一个网站时，网络服务商能够利用 Cookie 对用户活动进行识别。〔25〕在“Cookie 同步”过程中，不同网络服务商使用的大量“第三方 Cookie”被链接起来，从而使用户的个人信息在多个平台上传播。〔26〕

（二）经济激励使去匿名化具有针对性

大数据环境和无处不在的个人信息收集技术使去匿名化变得越来越可行，信息收集主体能够获得更多的辅助信息对匿名化信息进行识别。对于网络服务商、广告商而言，重新识别用户个人信息有利于产品与服务的定向营销，存在强大的经济激励。随着去匿名化成为一项可行且有利可图的措施，重新识别匿名化信息的风险也在增加。

1. 去匿名化个人信息有利于定向营销

阿瑟·米勒早在 1971 年就提出计算机化将允许“包括预测个人或群体行为的模拟活动”，警告未来可能会出现由组织利用计算机进行“人为操纵”，影响和塑造用户行为。〔27〕如今的数字和互联网技术使米勒预言成为现实，现代营销的目标是对个人进行有针对性的跟踪，以定制产品、服务和价格。定向营销已经成为跟踪和汇总用户个人信息的强大经济激励手段，与此同时，一个以收集、整合、识别和出售用户个人信息为唯一目标的完整行业正在形成。用户个人信息和网络

---

〔21〕 Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1723 (2010).

〔22〕 Federal Trade Commission, *Self-regulatory Principles for Online Behavioral Advertising*, *available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf*, *last visited on Sep.* 21, 2023.

〔23〕 See Matthew C. Keck, *Cookies, The Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 Albany Law Journal of Science and Technology 83, 88 (2002).

〔24〕 See Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 University of Chicago Law Review 261, 262 (2008).

〔25〕 See Matthew C. Keck, *Cookies, The Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 Albany Law Journal of Science and Technology 83, 89 (2002).

〔26〕 See *Cookie Synching*, *Krux*, available at http://www.kruxdigital.com/broadcasts/krux_blog/cookie_synching/, last visited on Sep. 17, 2023.

〔27〕 See Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers*, University of Michigan Press, 1971, pp. 42－43.

活动处于网络服务商的“监控”之下，施奈尔提出：“监控是互联网的商业模式。每个人都处于许多公司的监控之下，从脸书公司这样的社交网络到手机供应商，这些数据被收集、编译、分析，并用于试图向我们出售产品。”〔28〕网络服务商从社交媒体账户、公共空间记录、消费者购买数据和网页浏览活动中收集大量信息，在信息主体不知情的情况下整合这些信息并进行识别，继而转售或进行定向营销。对匿名化信息的收集、使用等活动受到法律的豁免保护，导致存在一个基本上不受监督且利润很高的行业，使个人信息遭受极大的侵害风险。

定向营销对匿名化信息的重新识别包括两种模式，即与线下信息的融合以及与过去信息的融合。杰弗里·切斯特提出：“在互联网时代，广告商正在开发越来越复杂的技术来跟踪、分析和说服我们。”〔29〕营销人员将线上收集的匿名化信息与线下信息相结合，即使用户只提供匿名化信息，其也能够交叉参考各项线下信息获得用户的真实房产信息、家庭收入、婚姻状况、联系电话等个人信息。例如，广告商采用精确的流程专注于更小的人群（例如对某小区的居民进行识别），根据线上获得的匿名化信息对应线下接触的具体客户（例如根据线上提供的停车位号码找到小区居民的居住详细地址与使用的汽车品牌等），由于信息主体倾向于在线上提供模糊信息而在线下提供真实信息，广告商能够快速锁定潜在客户并进行定向广告的投放。与过去信息的融合主要表现在网络空间中，网络服务商存储大量用户过去信息，“并能够在未来匹配更多的有价值信息”〔30〕。即使法律要求不得收集个人真实敏感信息或未经用户明确同意不得收集个人信息，但是网络服务商已经在先获得大量可识别信息，导致用户仅提供匿名化信息时网络服务商也可以轻易进行去匿名化操作从而获利。

2. 去匿名化个人信息具有数字资产属性

个人信息具有数字资产属性，当网络服务商或其他持有者无法正常运转时，个人信息将作为一种资产进行处分。例如，网络零售商爱儿玛公司（Toysmart）制定非常严格的隐私政策保护客户个人信息，但是当其破产时，这些客户信息将作为资产出售给其他公司。〔31〕虽然网络服务商等个人信息处理者向用户承诺妥善保管个人信息并进行匿名化处理，如《腾讯隐私政策》“存储信息的期限”项下规定“当我们的产品或服务发生停止运营的情形时，我们将采取例如，推送通知、公告等形式通知您，并在合理的期限内删除或匿名化处理您的个人信息”，但是该隐私政策同时在“第三方数据处理及信息的公开披露”项下规定“随着我们业务的持续发展，当发生合并、收购、资产转让等交易导致向第三方转移您的个人信息时，我们将通过推送通知、公告等形式告知您相关情形，按照法律法规及不低于本隐私政策所要求的标准继续保护或要求新的管理者继续保护您的个人信息”〔32〕。也就是说，当业务发生变化或为了更好的发展时，腾讯公司极有可

〔28〕 Liz Mineo, *On Internet Privacy, Be Very Afraid*, available at https://today.law.harvard.edu/internet-privacy-afraid/, last visited on Aug. 20, 2023.

〔29〕 Jeff Chester, *Digital Destiny*, The New Press, 2007, p. 128.

〔30〕 Bridget Small, *FTC Report Examines Data Brokers*, available at https://www.consumer.ftc.gov/blog/2014/05/ftc-report-examines-data-brokers, last visited on Oct. 11, 2023.

〔31〕 See Patrick F. Gallagher, *The Internet Website Privacy Policy: A Complete Misnomer?*, 35 Suffolk University Law Review 373, 375 (2001).

〔32〕《腾讯隐私政策》，载 https://privacy.qq.com/policy/tencent-privacypolicy，最后访问时间：2023 年 9 月 3 日。

能对已经匿名化的个人信息进行重新识别并向第三方转移。尽管腾讯公司向用户保证即使发生个人信息的流转也会要求新的管理者进行妥当保护，但事实上该规定仅具有宣示性作用而难以体现规范性效果，且由于用户对网络虚拟世界的陌生以及专业技能的匮乏，当其个人信息受到侵害时也无法及时寻求阻止与救济。

（三）用户依赖使去匿名化具有规模性

网络深度参与到现实生活中使无处不在的个人信息收集成为可能，例如商场、餐厅、游乐场等商家大量使用智能网络技术收集用户的面部照片、电话号码、地理位置和其他个人信息，以满足对便利服务的持续连接需求。用户向网络服务商提供信息不断常规化并具有规模性，一方面由于用户对自身个人信息的保护意识薄弱而主动提供大量信息甚至包括未匿名化的真实个人信息以换取便利和折扣优惠，另一方面由于长期使用相同网络服务或产品而导致放弃成本过高，用户不得不继续提供相关信息。

1. 用户主动依赖

随着从智能手机、健身追踪器到搜索引擎和地理位置跟踪应用程序的各种技术提供令人“着迷”的便利性，例如智能手机中网上预订与智能评价等应用程序为用户节约大量时间与精力，人们“似乎越来越愿意为了便利而放弃基本的隐私，并‘勉强’接受被公司监控的事实”〔33〕。美国皮尤研究中心（Pew Research Center）评估用户能够在多大程度上提供个人信息以换取某些交易折扣，发现“在各种情况下，许多美国人会分享个人信息或允许监控，以换取他们认为有价值的东西”〔34〕。可见，为了获得更大的便利性或是眼前利益，大量用户愿意提供未被匿名化的个人信息，导致其他场景下的匿名化信息与这些个人信息交叉从而被重新识别，或是其他只提供匿名化信息的用户由于与提供真实个人信息的用户在时间或空间上重叠而被去匿名化，从而形成个人信息集合。例如，早在2007年，美国得克萨斯州的两名研究人员已经利用少量的真实信息对网飞公司（Netflix）公开发布的用户电影评级匿名数据库进行重新识别。〔35〕只要少量用户提供真实个人信息，信息中介等具有去匿名化技术的实体就能够利用信息之间的联系以及时空因素对其他匿名化信息进行重新识别。

2. 用户被动依赖

《中华人民共和国消费者权益保护法》（2013年修正）第9条规定“消费者享有自主选择商品或者服务的权利”，但是，当用户长期使用某一智能手机应用程序或其他网络产品时，由于已经形成对所提供服务的依赖，所谓享有“选择使用或退出”的权利并不现实。〔36〕用户最初使用某一网络产品或服务时只是关注当下或短期利益，而不是未来或长期利益，这种短视或可称为“现

〔33〕 Liz Mineo, *On Internet Privacy, Be Very Afraid*, available at https://today.law.harvard.edu/internet-privacy-afraid/, last visited on Aug. 20, 2023.

〔34〕 Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, available at http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/, last visited on Jul. 14, 2023.

〔35〕 See Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *Proc. of the 29th IEEE Symposium on Security and Privacy*, available at http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, last visited on Sep. 18, 2023.

〔36〕 参见夏庆锋：《网络空间个人信息保护的通知义务完善与动态匿名化》，载《江汉论坛》2022年第3期。

实偏爱”的做法导致用户对网络服务商提供的产品或服务产生行为锁定，当行为主体的行为因习惯、组织学习或文化而“陷入”某种低效或次优状态时，行为锁定就会发生。〔37〕虽然用户对收集信息的去向可能感到不满，但是由于被动依赖性已经形成，且网络服务商作出承诺进行匿名化处理等安慰措施，使得个人信息收集、存储的现象愈发普遍。正如前文所述，即使网络服务商对个人信息进行匿名化处理，但是当其出售给广告商等其他信息中介时，信息接收者为了实现个人信息所具有的资产价值势必进行去匿名化处理。社会活动需要人们使用智能手机、申请电子邮箱与注册社交媒体账户，而随着现实社会适应技术创新并更加依赖技术的便利，作为弱势的普通用户只能不断出让个人信息利益，使信息中介持续获得数量巨大的去匿名化个人信息。

三、禁止去匿名化措施存在不足

个人信息的匿名化过程通常会删除直接标识符与间接标识符，但是一般不会删除准标识符（指不具有识别性，但可以与其他信息合并后产生链接性以帮助识别信息主体的信息内容），一方面原因在于准标识符不具有与直接标识符或间接标识符同等的可识别属性，另一方面则因为准标识符传达的内容有利于保持信息效用，防止信息的价值减损过大。〔38〕例如，受教育程度、收入区间、宗教信仰等信息不具有与姓名、身份证号码、单位等信息相同的识别性，但当这些信息在特定上下文语境中或与其他信息合并时，则能够对应至特定的信息主体。然而，正是由于准标识符的存在使完美匿名化难以实现。欧盟第 29 条数据保护工作组在其发布的 05/2014 号意见书《关于匿名化技术的意见》中也提出：“在本意见书中，工作组使用‘匿名化技术’这一概念，而非‘匿名性’或‘匿名数据’，从而指出任何旨在将数据匿名化的技术和组织措施对于数据被再识别所引致的固有剩余风险。”〔39〕虽然网络服务商等信息中介在隐私政策或用户协议中承诺保护用户个人信息并进行匿名化处理，信息发出者与信息接收者订立合同约定不得进行去匿名化操作，甚至立法中直接规定去匿名化禁令，但这些措施皆无法有效禁止去匿名化，使信息主体承受各种去匿名化风险与直接侵害。

（一）网络服务商承诺不具有广泛效力

网络服务商为用户提供记录与发布个人信息的平台，但由于去匿名化技术的不断发展以及识别者能够获得大量公共信息，即使网络服务商承诺进行匿名化保护也极有可能被他人识别。〔40〕前述网飞公司匿名数据库识别案例中所使用的辅助信息完全来源于网络中的公共信息，大量公共信息的存在使匿名化信息转变为个人信息具有可能，增加去匿名化风险。以一款名为耳语（Whisper）的匿名社交网络应用为例。耳语自称是互联网上“最安全的地方”，然而它的使用条款已经演变成讲述“一个更真实、更不可靠的关于匿名化的故事”。《耳语隐私政策》规定：“我

〔37〕 参见夏庆锋：《网络合同中不正当格式条款的纠正规则》，载《江淮论坛》2020 年第 2 期。

〔38〕 参见高富平：《个人信息流通利用的制度基础——以信息识别性为视角》，载《环球法律评论》2022 年第 1 期。

〔39〕 Article 29 Data Protection Working Party 0829/14/EN WP216, *Opinion* 05/2014 *on Anonymisat-Ion Techniques*, available at http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, last visited on Sep. 19, 2023.

〔40〕 See Jane Yakowitz, *Tragedy of the Data Commons*, 25 Harvard Journal of Law & Technology 1, 25-26 (2011).

们收集很少的可以用来识别您个人的信息，……我们的目标是为您提供一种工具，让您在保持匿名的情况下表达自己。然而，请记住，您在 Whisper 将是公开可见的，所以如果您想保持匿名，您不应该在您的 Whisper 中包括任何个人信息，……即使您在 Whisper 中不包含个人信息，您对服务的使用仍可能使他人随着时间的推移，根据您的 Whisper 内容以及您的大致位置确定您的身份，……”〔41〕该条款显示出网络服务商承诺的不可靠性，无法产生约束其他信息接收者不进行去匿名化活动的广泛效力，即使网络服务商采取措施阻止去匿名化操作，识别者仍然可以根据一些基本的信息进行重新识别。

网络服务商承诺无法对抗“蓄意侵入者”的攻击，在“西北纪念医院诉阿什克罗夫特案”（Northwestern Memorial Hospital v. Ashcroft）中，理查德·波斯纳法官敏锐地观察到匿名化信息容易被重新识别。〔42〕政府要求信息主体提交部分接受堕胎手术的妇女病历，为了不泄露这些妇女的身份，其中涉及个人信息的内容将被删除。〔43〕法院认为，虽然对相关个人信息进行删除，但前述病历仍然侵犯妇女的隐私权，因此撤销政府的要求。〔44〕波斯纳法官认为：“这些女性中的一些人会担心，当她们被涂黑的记录成为纽约审判记录的一部分时，她们的熟人或熟练的‘谷歌人’对每个病人的病史和性记录进行筛选，就能把 45 名女性‘排除’出来，从而使她们遭受威胁、羞辱和谩骂。”〔45〕波斯纳法官虽然仅使用“熟练的谷歌人”这一简单词汇，但实际上概括出现代网络技术对个人信息的深度挖掘能力，能够对已经匿名化的个人信息进行检索与分析，并将其与其他信息联系以进行去匿名化处理。《谷歌隐私权政策》规定“我们不会与广告主分享可用于识别您个人身份的信息，例如您的姓名或电子邮箱地址”，虽然谷歌公司承诺不针对匿名化信息进行去匿名化处理，但谷歌平台是一个开放式平台，其他用户或公司完全可以利用谷歌搜索与分析技术对匿名化信息进行重新识别。〔46〕因此，即便谷歌等网络服务商承诺保护用户个人信息并进行匿名化处理，但利用大量公共资源的便利性使他人能够轻松进行去匿名化操作，导致个人隐私与人格利益等遭受侵害。

（二）合同义务约定无法发挥制约作用

美国一些州的法律采用匿名化标准，要求监管实体公开承诺以匿名化形式维护信息，且不得重新识别信息，同时对信息接收者施加“下游合同义务”，即匿名化信息接收者同意遵守与监管实体相同的数据保护要求。例如，《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）、《弗吉尼亚州消费者数据保护法案》（Virginia Consumer Data Protection Act，VCDPA）、《科罗拉多州隐私法案》（Colorado Privacy Act，CPA）、《信息透明与个人数据控制法案》（Information Transparency and Personal Data Control Act，ITPDCA）等法律都采用“公共承

〔41〕 Paul Lewis & Dominic Rushe，*Revealed：How Whisper App Tracks “Anonymous” Users*，available at http://www.theguardian.com/world/2014/oct/16/-sp-revealed-whisper-app-tracking-users，last visited on Dec. 20，2022.

〔42〕 See Northwestern Memorial Hospital v. Ashcroft，362，F. 3d 923，929（7th Cir. 2004）.

〔43〕 See Northwestern Memorial Hospital v. Ashcroft，362，F. 3d 923，925（7th Cir. 2004）.

〔44〕 See Northwestern Memorial Hospital v. Ashcroft，362，F. 3d 932－933（7th Cir. 2004）.

〔45〕 See Northwestern Memorial Hospital v. Ashcroft，362，F. 3d 929（7th Cir. 2004）.

〔46〕 参见《谷歌隐私权政策》，载 https://policies.google.cn/privacy?hl=zh-CN&gl=cn，最后访问时间：2022 年 11 月 9 日。

诺＋合同义务”的匿名化标准。〔47〕合同义务要求匿名化信息接收者遵守其与信息发出者的约定，不得对匿名化信息进行去匿名化处理。但是，重新识别完全可以在“阴影”中发生。例如，网络服务商将其持有的用户个人信息集进行匿名化并出售给营销公司，网络服务商与营销公司订立合同约定不得对匿名化信息进行去匿名化处理，尽管营销公司作出承诺不会重新识别匿名化信息，但面对可能带来的巨大利益，且进行去匿名化处理时网络服务商无法得知或进行干预，合同义务的约定难以发挥制约作用。虽然信息接收者负有妥善保管匿名化信息的义务，但其完全能够秘密地进行重新识别，不仅网络服务商与其他监管机构无法察觉，而且作为受害人的信息主体也难以找到实际过错方。

合同义务约定无法发挥制约作用的另一个因素在于其不能成为具有严格制约效力的规范。例如，当下游信息接收者是一个旨在促进公权力完善、提高社会管理效率或是进行科研创新的研究机构时，将如何适用合同义务的约定？此时作为促进社会进步的研究人员是否仍需遵守匿名化规定而不得获取更为详细的信息背景资料？域外立法对此已有规定，例如美国《健康保险携带和责任法案》中的隐私规则规定，如果任何一方在加州居住或经营，则附带健康隐私信息的销售或许可合同必须声明：（1）交换的匿名化信息包含匿名化的患者数据；（2）根据 CCPA，重新识别和试图重新识别是被禁止的；（3）除非法律另有要求，只有在第三方受到同等或更严格条件的合同约束下，接收者方可重新披露已去除身份的信息。〔48〕该规则强调当“法律另有要求”时接收者可以对匿名化信息进行重新识别，也就是说，当研究人员为了公共利益收集匿名化信息并进行去匿名化处理时符合前法要求而无需遵守不得重新识别的合同义务约定。虽然合同明确约定不得重新识别匿名化信息，但只要接收者提出“合理理由”即可轻易违背合同义务且不受追责，这极大地抵消不法识别者的违约成本。例如，新冠疫情期间部分医疗服务平台违背与用户的匿名约定，以“公共利益”“义诊”等为理由对匿名化医疗信息进行去匿名化并用于广告推送、用户画像和信用评价等商业活动，使个人信息权益遭受损害。当更多的下游信息接收者提出“合理理由”进行去匿名化操作时，必然导致合同义务约束去匿名化不再可行。

（三）立法直接禁止难以实现规制效果

有学者提出通过直接立法对去匿名化行为进行禁止，规定个人信息经过匿名化处理后信息管理者需要向信息主体作出承诺保护各项权益，如果出现重新识别的情形时则向有过错的信息管理者和信息识别者追究法律责任。〔49〕域外立法已有相关措施，例如美国《加州健康与安全法规》（California Health and Safety Code，CHSC）规定“在任何情况下，医院、缔约者或次缔约者均

〔47〕 See Cal. Civ. Code § 1798.140 (m) (2)—(3) (2021); VA. Code Ann. § 59.1-575 (2021); Colo. Rev. Stat. § 6-1-1303 (11) (b)—(c) (2021); Information Transparency & Personal Data Control Act, H. R. 1816, 117th Cong. § 7 (6) (C)—(F) (2021).

〔48〕 See Nick Weil, *The De-identification Dilemma: When HIPAA Entities Become CCPA Subjects*, 24 Journal of Health Care Compliance 47, 48 (2022).

〔49〕 See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1758 (2010). 国内也有学者提出立法中应明确禁止数据使用人以任何目的从事身份再识别行为，并追究从事再识别行为主体的法律责任。参见金耀：《个人信息去身份的法理基础与规范重塑》，载《法学评论》2017 年第 3 期；齐英程：《我国个人信息匿名化规则的检视与替代选择》，载《环球法律评论》2021 年第 3 期。

不得重新确认或试图重新确认根据本节收到的任何信息”〔50〕，美国《统一个人数据保护法案》（Uniform Personal Data Protection Act，UPDPA）也规定，通过重新识别或导致重新识别假名数据或去标识化数据来收集或创建个人数据被视为“禁止的数据实践”。〔51〕立法者试图通过去匿名化禁令解决后顾之忧，防止去匿名化对信息主体造成损害，然而实践中禁止去匿名化的规制效果并不理想。美国《加州健康与安全法规》仅规定医院与缔约关系人不得进行去匿名化处理，而承受去匿名化风险的患者更加担心他们的匿名化信息被技术公司、非临床研究团队、新闻记者、非专业社区成员和其他非健康行业参与者重新识别。美国《统一个人数据保护法案》虽然包括全面禁止数据重新识别的内容，但同时规定除外规则，即“（a）重新识别是由之前进行假名或去标识化的控制者或处理者执行的；（b）数据主体希望进行重新识别的控制者以识别的形式持有其个人数据；（c）重新识别的目的是评估去标识化数据的隐私风险，进行重新识别的人不得使用或披露重新识别的个人数据，除非向创建去标识化数据的控制者或处理者证明隐私漏洞”三种情况可以对匿名化数据进行重新识别。〔52〕前述（b）项规定“数据主体希望进行重新识别”的情形下可以进行去匿名化处理，但实践中网络用户很少直接向网络服务商提出要求希望将匿名化的信息进行去匿名化处理，这种处理方式对于用户并无利益可言，反而有利于网络服务商进行有针对性的营销或作为数字资产的一种。因此，网络服务商完全可以通过各种形式使用户作出非真实内心意思的同意表示，继而进行去匿名化处理，导致立法禁令形同虚设。〔53〕日本《个人信息保护法》与英国《新数据保护法案》（New Data Protection Bill）也有禁止去匿名化的规定，但去匿名化过程本身具有的隐蔽性以及立法上对匿名化信息的在先豁免规定使规制效果并不明显。而且，即使立法能够根据匿名化情况制定具体措施，但是由于法律法规的起草与实施需要的周期较长，当法律予以公布时去匿名化技术已经发展到新的阶段，立法措施仍然难以发挥较好的规制作用。

事实上，有些法律已经放弃直接禁止去匿名化的规制模式，而是进行妥协。美国《健康保险携带和责任法案》隐私规则允许所规制的实体重新识别匿名化的健康信息，规定采用分配一个代码或其他记录标识的方法来允许被标识的信息被规制实体重新识别，只要（1）记录识别手段不是“源自”关于数据主体的信息或以其他方式能够被“翻译”以识别数据主体，以及（2）规制主体没有“为任何其他目的”使用或披露记录识别手段或是披露重新识别的机制。〔54〕该隐私规则明确指出，如果已经匿名化的信息被重新识别，受法律规制实体对信息的使用和披露必须遵守隐私规则的要求。〔55〕前述隐私规则对于去匿名化措施的妥协具有实际意义，但要求重新识别匿名化信息的主体遵守数据保护法律的规定不具有可期待性。对匿名化信息进行重新识别本身具有隐蔽性，网络服务商或广告商等其他信息中介难以主动承担法律所规定的义务内容，且作为信息

〔50〕 Cal. Health & Safety Code § § 128766 (b) (2021).

〔51〕 See Cason Schmit, Brian N. Larson & Hye-Chung Kum, *Data Privacy in the Time of Plague*, 21 Yale Journal of Health Policy, Law & Ethics 152, 202 - 208 (2022).

〔52〕 See Cason Schmit, Brian N. Larson & Hye-Chung Kum, *Data Privacy in the Time of Plague*, 21 Yale Journal of Health Policy, Law & Ethics 152, 208 (2022).

〔53〕 参见夏庆锋：《网络合同格式条款提示说明义务的履行瑕疵与完善措施》，载《清华法学》2022年第6期。

〔54〕 See 45 C. F. R. § 164.514 (c).

〔55〕 See 45 C. F. R. § 164.502 (d) (2) (i)—(ii).

主体的用户已经确认个人信息将以匿名化的方式保存或作其他使用，更无及时发现匿名化信息被重新识别的敏感性和必要专业知识。

四、基于动态匿名化的增强保护

匿名化措施能够隐蔽或删除可识别信息从而降低流动信息与对应主体的可链接性，防止对信息主体的直接识别，应该受到鼓励。但是，由于各种去匿名化技术的出现与升级，重新识别匿名化信息的风险不断升高。考虑到信息收集的普遍性，以及信息中介重新识别匿名化信息的强大经济动机，我国《个人信息保护法》试图使用静态的匿名化制度界分匿名化信息与非匿名化个人信息并适用不同保护措施存在不足。静态匿名化倾向于制造一种明确和永久轮廓的泡影，假设一旦个人信息被匿名化则无法链接至信息主体，不仅初始个人信息处理者可以不再顾及，而且信息接收者也没有任何保护义务或责任。实际上并非如此，静态匿名化只是一种暂时的状态，当匿名化信息放在不同语境下或与不同的信息集交叉时将被重新识别。由于创建完美的匿名化信息难度很大，应该采用动态的方法对去匿名化风险进行定期评估，包括对匿名化信息可能造成的损害与匿名化信息所在语境的变化等因素进行分析。〔56〕动态匿名化方法与静态匿名化的一次性标准不同，是一种持续性的规范措施，更加关注基于流程的规制而非仅仅关注基于结果的规制。例如，动态匿名化能够根据匿名化信息所包含的具体信息及相关内容来判断去匿名化风险的高低以及是否需要重新匿名化，包括对信息唯一性、信息敏感度、信息处理者类型、信息用途、信息处理技术等因素的考察。当匿名化信息不具有唯一性时，此时去匿名化风险较低，即使具有某些非直接识别符也不会对信息主体造成损害，而当匿名化信息具有高度唯一性时（例如国内排名前 2 的高校大学生月平均生活费的匿名化信息），则较为容易进行重新识别，需进行严格的匿名化处理与动态监督。又如，健康、金融等个人信息具有较高敏感性，需要利用动态匿名化标准进行界分并实时评估损害风险，且当匿名化信息处理者为网络服务商等商业主体时也需采用严格的动态匿名化方法，防止对个人产生信息权益的损害风险甚至现实损害。此外，在商业主体的匿名化信息处理行为同样导致对个人产生较大的损害风险以及信息匿名化处理技术不彻底等情形下，亦需进行严格的动态匿名化测试，从而实现匿名化制度对个人信息权益的增强保护。

（一）动态匿名化关注可能损害

动态匿名化更加关注匿名化信息被去匿名化的风险以及由此给信息主体造成的损害。匿名化信息与非匿名化个人信息之间的界限不应当是固定的，在某一个时期内匿名化信息的利用不会对信息主体造成损害，则此时无需进行保护，而在另一个时期内技术的发展使去匿名化成为可能甚至已经实际造成损害，则需要进行再匿名化处理。只要匿名化信息的利用行为存在损害风险，就不能认定为完全匿名化，需要根据具体的使用情况采取措施。英国信息专员办公室（Information

〔56〕 有学者提出应当将风险管理理念嵌入个人信息匿名化的法律制度构建中，实际上也反映出一种动态化的观点。参见张丽、许多奇：《风险控制理念下我国个人信息匿名化处理的法律规制》，载《重庆大学学报（社会科学版）》2023 年第 2 期。

Commissioner's Office，ICO）在其早期发布的匿名化规则中已经尝试使用基于损害风险的方法，提出当受到损害的风险越高时，应采取的程序措施就越严格，反之亦然。〔57〕上海市数据交易中心2016年出台的《流通数据处理准则》也有对隐私风险的持续关注，其中第3条第8款规定："数据持有人应对数据流通的隐私风险进行评估，确保流通涉及的个人数据处理和服务符合数据和隐私保护要求。"但是，对可能损害的分析存在认定困难，损害在隐私法中是一个有争议的概念，实践中"许多损害都是渐进的，或者难以量化和阐明，甚至需要等到事实发生多年后才会被发现"〔58〕。由于去匿名化过程本身具有隐蔽性，而判断损害的发生依赖于建立法律上认可的因果关系，去匿名化过程与损害存在直接、明确的因果关系较难论证。因此，为了保护用户个人信息与隐私权益不因个人信息泄露而遭受损害，且由于网络环境的开放性与瞬时性等特征造成的损害无限放大，应在确定匿名化信息的不当使用与用户损害存在相当因果关系时即认定个人信息匿名化不完全并进行再匿名化处理。

动态匿名化对去匿名化风险与可能造成损害进行动态分析，体现为一种基于过程的安全方法，有利于将匿名化从单一的静态目标转变为动态化的程序设计。根据动态匿名化的要求，当匿名化信息的利用不会对信息主体造成损害时，应当进行豁免，允许网络服务商等信息中介进行任意使用。也就是说，当且仅当某些保障措施到位时，将匿名化信息置于《个人信息保护法》的保护范围之外，这不仅与确保信息主体权利得到强有力和系统的保护兼容，而且与确保基于"合法性""数据最小化""目的限制"等原则利用匿名化信息相契合。〔59〕只有当匿名化信息存在侵害信息主体权益的风险甚至造成实际损害时，动态匿名化才要求个人信息处理主体以及匿名化信息发出与接收主体承担再匿名化责任。正如有学者提出，我国《个人信息保护法》需要解决问题的实质不在于技术上能否匿名，而在于如何在制度上保证其不被再识别，动态匿名化方法的加入会促使该目标所实现。〔60〕

（二）动态匿名化结合上下文语境

个人信息除了具有可识别性的关键特征外，还具有相关性属性。所谓相关性，是指当单独观察某一信息不能对应至信息主体时，可放在上下文语境中发现其内在含义，例如我国《个人信息保护法》第4条规定个人信息是与自然人"有关的各种信息"。欧盟第29条数据保护工作组在其关于个人信息的概念中也涉及相关性概念，将个人信息分为四个部分，分别是"任何资料""有关""确定的或可辨认的""自然人"，并提出一个包括"内容元素、目的元素与结果元素"三管齐下的测试方法，以确定是否与自然人有关。〔61〕内容元素指个人信息中直接包括个人的身份信息，如护照号码、驾驶证号码等；目的元素指信息本身并不包含个人身份信息，但是个人信息的

〔57〕 See Derek du Preez, *ICO Under Fire for Dropping BT Data Breach Probe*, available at www.computing.co.uk/ctg/news/2023566/ico-dropping-bt-breach-probe, last visited on Apr. 1, 2023.

〔58〕 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Washington Law Review 703, 730 (2016).

〔59〕 See Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, 34 Wisconsin International Law Journal 284, 310 - 311 (2016).

〔60〕 参见张新宝：《我国个人信息保护法立法主要矛盾研讨》，载《吉林大学社会科学学报》2018年第5期。

〔61〕 See Article 29 Data Protection Working Party, *Opinion* 04/2007 *on the Concept of Personal Data*, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm, last visited on Jun. 12, 2023.

使用目的在于“评估、以某种方式操纵或影响个人的地位或行为”；结果元素指对个人信息的使用结果将对个人的权利与利益产生影响。〔62〕尤其在目的元素与结果元素测试下，个人信息与匿名化信息的界限是动态的，某些语境下的匿名化信息具有匿名化效果，而另一些语境下的匿名化信息虽然也删除与个人的联系要素，但一旦结合上下文仍然可以对应到信息主体以及对信息主体产生影响。马克·艾略特认为“数据是否为匿名的取决于该等数据与其环境之间的关系”，当匿名化信息的语境发生变化时，该信息能够再次成为具有识别性的个人信息。〔63〕所谓的匿名化仅具有相对性，在不同语境下表现为不同面向，当在某些语境下无法识别的匿名化信息转换至其他语境时将成为可以识别特定个人的非匿名化个人信息，匿名化信息与非匿名化个人信息具有一体两面的关系，二者可以相互转化而非决然对立。

考虑到匿名化信息与个人信息在具体语境中的转换效果，应当采用动态匿名化方法。例如，在时间点 N，个人信息已经令人满意地进行匿名化处理，此时并无隐私侵害与去匿名化的风险。但是，在时间点 N+1，虽然匿名化信息自身没有发生变化，但由于所在的上下文语境加入更多辅助信息，此时利用匿名化信息将导致信息主体被重新识别、“评估、以某种方式操纵或影响个人的地位或行为”或是将对个人权益产生影响，那么该匿名化信息则转化为具有识别性的个人信息，需要进行再匿名化处理。置于不同语境下的匿名化信息产生去匿名化的风险不同，因此采用“一刀切”的静态匿名化方法要么导致保护过度，要么使得保护不足，无法产生较好的规制效果。动态匿名化方法结合上下文语境，即使匿名化信息通过分析内容本身无法涉及具体个人，只要对其使用能够根据上下文找到信息主体或对信息主体产生影响甚至实际损害，就应禁止继续使用该信息并进行更为严格的匿名化处理。

（三）动态匿名化符合比例原则

比例原则调整手段与目的之间的理性关系，为权力与权利的行使提供合理尺度，具有目的正当性、适当性、必要性与均衡性特征，其最初虽为行政法原则，但在个人信息保护法中同样可以适用。各国个人信息保护立法已经体现对比例原则的尊重，例如欧洲理事会于 1981 年公布的《个人数据自动化处理中的个人保护公约》第 5 条规定“数据处理应与追求的合法目的相称，并在处理的所有阶段与所有关联的利益之间反映一种公正平衡，不论公利还是私利，以及所关涉的权利和自由”“正在处理中的个人数据应当：……对于其处理目的，适当、关联且不过量；……以允许数据主体识别的形式保存，不超过实现该等数据处理的目的所需的时间”〔64〕，欧盟《通用数据保护条例》序言第 4 条规定“个人数据的处理应服务于人类。保护个人数据的权利不是绝对权利，须结合考虑其社会功能并依据比例原则与其他基本权利保持平衡”〔65〕，我国《民法典》第 1035 条第 1 款规定“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理”，我国

〔62〕 See Article 29 Data Protection Working Party, *Opinion* 04/2007 *on the Concept of Personal Data*, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm, last visited on Jun. 12, 2023.

〔63〕 参见张建文、高悦：《我国个人信息匿名化的法律标准与规则重塑》，载《河北法学》2020 年第 1 期。

〔64〕《欧洲理事会个人数据自动化处理中的个人保护公约》，载 https://wenku.baidu.com/view/f25014713f1ec5da50e2524de518964bcf84d2d0.html，最后访问时间：2023 年 5 月 11 日。

〔65〕 中国信息通信研究院互联网法律研究中心、京东法律研究院编：《欧盟数据保护法规汇编》，中国法制出版社 2019 年版，第 12 页。

《个人信息保护法》第6条规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式”等。比例原则提倡均衡、禁止过度，体现对实质正义的追求，这也是动态匿名化平衡个人信息保护与个人信息效用的根本目的。〔66〕

动态匿名化不阻碍对匿名化信息的自由使用，但相对于目前立法规定的静态标准而言，动态的匿名化测试更加有利于对用户个人信息权益进行保护，体现目的正当性、适当性、必要性与均衡性的比例原则要求。当经过动态匿名化测试后的信息符合匿名化要求时，对该信息的利用行为具有目的正当性，其不会对个人信息主体造成损害；适当性指所采用手段有利于目的的实现，动态匿名化对匿名化信息采用更为严格的要求，虽然意在增强对信息主体的保护，但同时也提高了对个人信息的利用效率，符合平衡个人信息保护与个人信息效用的立法目的；〔67〕必要性指个人信息处理者应当在最小范围内以最低限度的方式收集和处理个人信息，而经过动态匿名化处理的信息已经删除各种具有识别性的标识符，甚至在特殊语境下删除具有联系的其他内容，符合比例原则的必要性要求；〔68〕均衡性主要体现在对公权力的约束，即使符合前述适当性、必要性要求，但如果促进公共利益的实现与对公共利益造成的损害不成比例，则违反均衡性，利用匿名化信息提高社会管理效率或是进行科学研究仍然需符合动态匿名化测试标准，若产生去匿名化风险甚至造成损害，则需进行更为严格的再匿名化处理。

五、结　论

个人信息保护与个人信息效用是相互冲突的两个目标。为了效用，匿名化信息不可完全删除所有个人与社会之间具有连接性的内容，而完全按照信息主体提供的个人信息进行发布虽然可以获得完美的效用，但将丧失所有隐私与个人信息权益，使信息主体面临受到各种侵害的风险。因此，对个人信息进行匿名化是平衡保护与利用的重要措施。然而，伴随网络技术的不断发展，技术进步、经济激励与用户依赖使匿名化信息与非匿名化个人信息的界限愈发模糊，虽然网络服务商承诺不进行去匿名化操作，信息中介也确立不得采用去匿名化操作的合同约定，甚至立法上已有直接规定的去匿名化禁令，但仍然无法阻止去匿名化现象的发生与愈发普遍。个人信息保护与利用领域没有完美匿名化措施，这也导致现行法对匿名化信息的豁免保护规定缺乏合理性，未能准确把握信息时代的客观风险。因此，为了适应现代网络社会快速发展的重新识别技术、完善对信息主体权益的保护、促进信息效用的发挥，应当关注去匿名化的潜在风险，采用更为现实、更具时效性的动态匿名化方法，从而改进现行立法的匿名化制度。动态匿名化是一种持续性的规范措施，防止对匿名化信息的一次性认定导致信息中介进行不正当却被法律所豁免的去匿名化操作，侵害信息主体的各项权益。因此，应将动态匿名化方法加入个人信息保护法中，使匿名化从单一的静态目标转变为动态化的程序设计，进而将去匿名化和敏感信息披露的成本提高到足具威慑力的水平。塞缪尔·沃伦与路易斯·布兰代斯提出的经典理性平衡观点认为“当信息具有社会

〔66〕 参见郑晓剑：《比例原则在民法上的适用及展开》，载《中国法学》2016年第2期。

〔67〕 参见梅扬：《比例原则的适用范围与限度》，载《法学研究》2020年第2期。

〔68〕 参见王道发：《个人信息处理者过错推定责任研究》，载《中国法学》2022年第5期。

价值时，隐私权不应干扰信息流动”〔69〕，本文提出的动态匿名化方法并非利用法律规定强制性地阻止匿名化信息自由流动，而是结合比例原则进行分析，在允许匿名化信息自由流动的同时增强对个人信息主体各项权益的保护。

Abstract：According to Article 73 of the China Personal Information Protection Law, anonymization refers to the process in which personal information cannot identify a specific natural person and cannot be restored after processing. Article 4 provides exemption protection for anonymized information and adopts static anonymization method to balance personal information protection and personal information utilization. However, with the rapid development of social informatization and network technology, the boundary between anonymized information and non-anonymized personal information tends to be blurred, and strong economic incentives make de-anonymized information targeted, resulting in the infringement risk and even real damage from the re-identified anonymized information to the information subject. Although the existing measures, such as ISP commitment, contractual obligation agreement and direct prohibition in legislation, restrict the risk of de-anonymization, they fail to achieve a good regulatory effect. Therefore, a more flexible dynamic anonymization method should be added to the existing anonymization system. When the use of anonymized information may cause damage or the change of context makes the anonymized information identifiable, more strict re-anonymization should be carried out. Otherwise, the information that is not truly anonymized still needs to be protected by law.

Key Words：personal information, anonymized information, de-anonymization, dynamic anonymization, proportion principle

（责任编辑：武　腾）

〔69〕 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harvard Law Review 193, 196－197 (1890).