网络空间个人信息保护的通知义务完善与动态匿名化

夏庆锋

摘要：我国《民法典》与《个人信息保护法》都对个人信息进行了规定并提出保护措施，对日益严重的个人信息滥用现象以及产生的对信息主体的侵害事实具有抑制作用，有利于对个人信息处理者收集、使用个人信息等行为进行监督和纠正。但是目前看，相关法律规定仍然存在保护困境，尤其在人们日常活动频繁的网络空间中，缺乏对用户选择同意权利的“名存实亡”与去匿名化信息处理行为对用户造成损害等问题的回应与解决。未来可增加完善网络公司等个人信息处理者的通知义务与动态匿名化的法律规定，要求网络公司履行条款内容的显著通知义务与重要事项的单独通知义务，同时采用根据匿名化信息可能被去匿名化及造成损害的风险评估对网络公司使用匿名化信息进行严格的程序性要求，并对已经造成损害的匿名化信息进行再匿名化处理。

关键词：个人信息；网络空间；保护困境；通知义务；动态匿名化

基金项目：国家社会科学基金重大项目“互联网交易制度与民事权利保护研究”（项目编号：20205011483）

中图分类号：D922.16　　文献标识码：A　　文章编号：1003-854X（2022）03-0095-09

《中华人民共和国民法典》（以下简称《民法典》）和《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》）都对个人信息进行了规定，具体到网络空间中，个人信息不仅包括用户姓名、出生日期、身份证件号码等内容，还包括用户登录网站进行的搜索查询、发送邮件、购买物品、下载软件、发布状态等一切活动中所留下的数据信息，以及通过这些信息推导出来的家庭环境、净资产、健康状况等衍生信息。网络空间个人信息具有高度识别性或聚合在一起产生明确的个人指向性，属于个人所有的信息权益，但由于这些信息存在于网络空间这一公共领域，容易被网络服务商、第三方平台等各类网络公司收集及使用。虽然网络公司也面临着收集、使用个人信息所获价值的不确定性，但由于个人信息处理行为的成本较低，而可能获得的收益非常大，这种成本收益的预期不对称性给予网络公司巨大的“激励效应”①。例如，网络公司通过将大量用户的个人信息与以往搜索信息相结合可提高交付给每个用户搜索结果的质量，从而获得更多用户登录其网站以提高广告业务的竞争力。②

网络公司处理个人信息的正当性源于其与用户订立的网络合同（包括《用户服务协议》《使用协议》等）及独自发布的隐私政策（包括《用户须知》等），虽然这些法律性文件已获得用户“知情”且“同意”，但基于网络空间的特殊性，例如网络公司不适当履行通知义务或利用提供更好的网络产品或服务来诱惑用户快速作出决定，导致用户草草同意甚至忽略有关个人信息的条款内容。近年来，网络公司处理个人信息的目的已经从单纯提升产品与服务质量逐步扩大到广告定位、销售个人数据（包括销售基于个人数据的预测模型）、操纵用户消费行为等，以至于产生“你不是顾客，你是产品”的现象③。这些不当收集与错误使用个人信息的行为不仅侵害用户的个人生活安宁，还将导致用户人身权益与财产权益遭受损害，例如基于身份信息泄露导致的虚拟财产盗窃、基于私密信息泄露导致的欺诈与歧视，甚至有些不法分子获知用户家庭地址

与行动轨迹后进行性骚扰、抢劫等严重的刑事犯罪。网络空间是人们日常活动的重要场所，对网络空间个人信息进行保护具有必要性与重要性，但由于存在网络用户同意表示的非真实性以及网络公司处理行为的不正当性等原因，加之现有立法措施并未进行妥善回应，导致法律层面对个人信息主体权益的保护功能难以实现。

一、网络用户同意表示的非真实性

取得用户真实同意应是网络公司处理个人信息的基本前提。例如，欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）规定数据主体有权同意或拒绝为一个或多个特定目的而处理其个人数据，美国《加利福尼亚州消费者隐私法》（California Consumer Privacy Act，CCPA）规定网络公司必须提供带有“请勿出售我的个人信息”字样的链接以保证消费者有权选择不出售自己的数据。但是，随着智能手机、健身追踪器、搜索引擎和地理定位追踪应用等产品与技术的发展，用户“似乎越来越愿意为了便利而不得不出让更多个人信息”。网络技术快速发展并不断渗透到用户的生活中虽然带来巨大价值，但这种普及化也导致“便利与隐私”的权衡问题[④]。在用户与网络公司订立的服务协议或网络公司提供的隐私政策中，有关收集、使用个人信息的条款虽然获得用户同意，但在网络空间这一特殊环境下，由于用户所固有的信息匮乏、有限理性特征以及锁定效应的作用，网络公司仍将有机可乘，利用个人信息的过度攫取行为对用户权益进行侵害。

（一）信息匮乏

用户同意网络公司处理其个人信息取决于这样一种假设，即用户分享个人信息的决定在于其充分知情网络公司的信息处理行为，从而作出真实的意思表示[⑤]。当用户不知情或缺乏重要的相关信息时，如不理解网络公司的服务协议或隐私政策的格式条款内容，则其不能作出有意义的决定，此时同意表示的功能价值就无法体现[⑥]。用户存在信息匮乏问题源于网络公司的错误陈述与隐瞒信息以及用户对网络技术缺乏了解，以至其获知与网络公司处理个人信息相关的信息成本过高甚至无法获知信息。对于用户而言，网络公司处理个人信息的行为通常是不透明的，尽管存在旨在告知用户各项处理行为的服务协议与隐私政策，但用户在获取、阅读这些格式条款时将面临极高的时间成本，且格式条款的内容通常是模糊、过于复杂的甚至可能随时更改，普通用户难以准确掌握。例如，一些网络公司向用户发送多个指向变更格式条款内容的超链接，使用户需要对不同格式条款进行排序，这种阅读义务的增加甚至导致用户无法确定更新内容。[⑦]网络公司通过混淆用户阅读服务协议以及隐私政策的内容来保护自己免受责任或掩盖产品某些不受欢迎的特性，直接导致用户对个人信息条款缺乏认知。

（二）有限理性

标准合同的法律假设认为，当事人在决定是否接受合同条款时，其行为是理性的[⑧]。但是，当这一理论代入网络空间时，却出现了新的问题[⑨]。网络空间与一般健康的市场环境不同，当用户决定是否加入某个特定的网络站点并同意其服务协议与隐私政策时，表现为有限理性。有限理性理论认为，由于人类的思维受到不完全信息和无法完全处理其拥有信息的限制，导致人类的决策不是完全客观和理性的。用户认知上的局限性与市场理论中“人类是理性行动者，在面对不确定性时作出理性的决定来最大化效用”这一假设相悖，网络空间尤其如此，虽然网络公司向用户提供其拟定的服务协议和隐私政策，但是在面对包含大量专业词汇的格式条款时，用户仍然无法完整阅读或理解所有内容。而且，网络公司往往在其网站上设置各种图片、视频等广告内容分散了用户注意力，使用户无法集中精力阅读或理解格式条款时就点击同意按钮。在这种有限理性的状态下，用户作出同意表示的真实性受到质疑。

市场经济下的竞争力量具有校正市场主体有限理性的作用[⑩]。竞争促使企业提供合适条款并更为消费者考虑，以获得行业内的比较优势，从而纠正消费者在有限理性情形下的次优决策。然而，这种效应在网络空间中难以产生，网络空间更多表现为“赢者通吃”的景象，垄断的趋势使竞争所能发挥的作用大受限制。[⑪]用户的有限理性导致其作出的同意决定不能反映真正的长期偏好。例如，行为经济学家认为，人类在评估风险时会遭受系统性的困难，即人类无法准确估计低概率、高成本伤害的预期成本，而网络空间个人信息的处理行为所产生的负效用正是“低概率、高成本伤害”的典型形式。[⑫]网络公司通常采用黑体、加粗、下划线等方式告知用户其个人信息的处理行为将在合法、透明的框架下进行，加之用户基于信息成本和认知局限的“乐观偏见”，确信其个人信息被错误使用并造成损害的事件难以发生[⑬]。而事实上，网络公司收集个人

信息后进行的各种处理行为无法为用户所预判，用户作出的同意表示并非知情将产生怎样的风险或者现实损害后的真实意思表示。

（三）锁定效应

用户长期使用网络公司提供的产品或服务将形成锁定效应，导致其难以通过从一个网络供应商、产品或服务转移到另一个网络供应商、产品或服务来表达他们的偏好。从对一种物品的使用转变到对另一种物品的使用，或是从一种办公系统向另一种办公系统变更，必然产生如更换物品的资金成本与处理新电脑、新手机而发生的转移电子文件或通讯录信息的时间成本。但是，在网络空间中，网络公司利用用户提供的个人信息进行整合和重新开发，将变更网络产品或网络服务的转化成本，升高到用户无法承担的程度。

信息密集型网络公司常常通过展示强有力的隐私保护措施，或者提供更多的“免费”产品或服务，来诱使用户进入“锁定状态”，如用户在使用微信（WeChat）时，微信公司将免费为用户提供云空间，以供其存储图片、视频等电子文件。但是，伴随使用时间的增加，用户再想将其多年累积的电子文件转移至钉钉（DingTalk）或其他即时通讯产品时几乎难以实现。这里的转移成本包括程序性转移成本、财务性转移成本以及关系性转移成本，程序性转移成本指更换网络产品或网络服务所必须付出的时间和精力成本，财务性转移成本包括会员福利、积分奖励等，而关系性转移成本则是指通过原来产品或服务所产生的各种网络关系将无法代入新的网络产品或服务中。当用户在某些网络服务商处投入大量的时间、精力和金钱成本后，其已经与网络公司形成牢固的锁定关系，更改产品或服务的成本将异常高昂。网络公司还利用其他方式锁定用户，如在用户将大量信息放至某一网络服务商处时，会因为各种“定制化产品和服务”被锁定在该产品上。锁定效应掩盖了用户的真实偏好，还会设置自由缔约障碍，使用户“被迫”同意网络公司变更的服务协议与隐私政策内容并继续使用其产品。

二、网络公司处理行为的不正当性

网络公司处理个人信息的实践行为主要包括以下几类：第一，利用所收集的个人信息作为生产工具来创建或优化产品、服务，例如百度公司（Baidu）使用用户的历史搜索数据来建议搜索词；第二，从市场研究或测试的角度推测用户偏好，例如对个人信息集合成的大数据进行分析，虽然不能具体到某一个用户，但基于同年龄段、同种职业、同一地区等相同因素可以对用户偏好进行较为准确的推测[14]；第三，定向广告或以其他方式影响用户偏好或选择，例如收集用户的职业、爱好等个人信息后针对性地推送广告，较为常见的是用户使用新浪微博（Sina Weibo）等网络产品时，在页面上将出现其可能感兴趣的广告信息；第四，汇总用户个人信息并作为数据产品出售给他人。网络公司收集、使用个人信息，无论是自有组织进行分析，或是通过第三方数据公司进行分析，还是仅仅收集个人信息并打包出售给其他公司，由于其在网络空间中具有优势缔约地位以及掌握的各项网络技术赋予其“迫使”用户作出同意表示的机会，使表面合法的处理行为具有不正当性。

（一）缺乏有效通知

只有用户“对网络公司的收集行为足够了解且可以对披露信息的风险和益处作出合理的评估”，此时才可以认定用户受到合理通知并作出真实同意的意思表示。[15]然而，网络空间中个人信息等数据的收集过程非常复杂，用户难以准确地跟踪收集到哪些信息、收集这些信息的目的、在哪些领域使用等内容，再加之网络环境不断变化、新颖的收集与分析工具层出不穷等因素，如果网络公司不进行有效通知，要求用户完全知情网络公司处理个人信息的行为几乎不能实现。[16]

网络公司提供的用户协议及隐私政策较为冗长、复杂，包含晦涩的专业用语和法律术语等内容，使用户无法在短时间内理解。许多网络公司还在用户协议中增加宽泛含义的语言以提供更大的灵活性，有利于在产生争议时进行获得更大利益或逃避应尽责任的变更解释。例如，在“俞某与浙江天猫网络有限公司等网络侵权责任纠纷案”中，俞某在线下实体店使用支付宝软件购买物品后，虽未同意“授权淘宝获取线下交易信息并展示”条款，但其仍然在手机淘宝App与天猫App中找到购买物品的交易信息。支付宝公司（Alipay）、淘宝公司（Taobao）、天猫公司（Tmall）提交了《支付宝隐私权政策》与《淘宝网隐私权政策》，分别载有“为了您可以正常使用支付宝服务，在下列情形下您需要向我们提供一些信息；我们也会在下列情形下向合法存有您信息的第三方收集您的信息”条款及“为展示您账户的订单信息，我们会收集您在使用我们服务过程中产生的订单信息用于向您展示及便于您对订单进行管理”条款并进行辩护，主张其收

集个人信息的行为具有法律依据。[17] 该案中，网络公司利用概括式的条款通知认为其已经履行适当的通知义务并获得用户同意，实际上为利用用户的不知情与使用产品的急切心理不正当地获取个人信息，网络公司对具体场景中收集个人信息的行为并未进行有效通知。虽然淘宝公司、天猫公司辩称在《隐私权政策》中对可能收集用户个人信息的情形已经进行提前告知和提示用户注意，但是其仍应在具体应用场景中再次取得用户同意，否则用户对个人信息的使用方式以及使用范围无法明确知晓，可能导致个人信息脱离用户意志而被不当收集和使用，不利于对个人信息的保护。

网络公司在收集个人信息后，还会将这些信息打包出售给数据经纪人等第三方数据公司，用户在不理解甚至不知情的情况下允许网络公司处理个人信息，此时更无法得知其个人信息被第三方数据公司收集和使用。从网络公司到数据公司，这种无穷尽的循环交付个人信息的行为使得用户根本无法监督其个人信息的使用情况，而作为最初获得个人信息的网络公司也不会充分告知用户个人信息的流向与使用范围。

（二）滥用个人信息

网络公司存在以不符合用户利益的方式使用个人信息。例如，脸书公司（Facebook）利用用户对“朋友网络系统”的信任诱使其分享更多信息，将超过 8700 万的用户数据泄露给数据分析公司“剑桥分析”（Cambridge Analytica），并被用来创建美国选民的档案，为 2016 年美国总统竞选预测提供数据支持。又如，有些针对性的广告推送并非用户希望获得的网络服务，且对用户隐私造成侵害。在“朱烨诉百度网讯科技有限公司 Cookies 隐私案”中，原告朱烨发现利用百度搜索引擎搜索相关关键词后，会在特定的网站上出现与关键词有关的广告，其认为百度公司在未经其知情和选择的前提下，利用网络技术记录和跟踪关键词，将其兴趣爱好、生活学习工作特点等显露在相关网站上，并利用记录的关键词对其进行广告投放，侵害了其隐私权。一审人民法院认为百度公司利用 Cookies 技术收集朱烨信息，并在朱烨不知情和不愿意的情形下进行商业利用，侵犯朱烨的隐私权。[18] 二审人民法院进行改判，认定“百度的个性化推荐行为不构成侵犯朱烨的隐私权”。[19] 百度公司利用已经掌握的用户个人信息和兴趣爱好，允许第三方网站根据这些数据向用户完美地推送广告，在很大程度上有利于第三方网站的业务发展。但是，虽然用户在使用百度服务之初就“默示同意”这种行为，而其本身并不知情，这种根据事先掌握的信息进行定向投放广告的针对性行为已经侵犯了用户的隐私权益。用户在使用百度服务进行互联网搜索时，百度公司提供技术的范围与搜索之后持续跟踪用户其他网络行为之间不存在必然联系，分析用户喜好和推送定制广告并不是一般网络用户所期望的合同履行内容。[20] 网络公司利用收集到的个人信息实施精准营销的行为严重危害用户的人格尊严并妨害人格的自由发展[21]。

网络公司滥用个人信息的又一趋势是价格歧视行为。当用户同意网络公司收集其个人信息时，用户行为将被网络公司制作成小标签，包括基本属性(性别、年龄、星座、身高、体重、腰围等)，购买能力（收入、是否有车、是否有房、购买力、消费信用水平等），行为特征（婚否、教育程度、家中是否有孕妇、是否有孩子、孩子性别、孩子年龄等），心理特征（活跃程度、颜色偏好、品牌偏好、促销敏感度、购物忠诚度等）等内容。这些个人信息被网络公司收集并计算用户对商品价格的接受区间，进而制定不同的价格。此外，网络公司的自动软件还会记录用户浏览某一类商品所花费的时间，如果用户花费时间较长，则自动软件将标识为对该类商品的价格敏感，界面会推荐性价比更高的商品；如果用户花费时间较短，网络公司的界面就会倾向于推荐价格较高的商品。

（三）形成安全风险

由于个人信息与信息主体之间的紧密联系以及实践中匿名化措施缺乏、匿名化效果不显著等原因，对个人信息的过度收集会带来更大的安全隐患。网络信息技术的快速发展为持续性收集具体的、广泛分布的个人信息提供支持，便于怀有不法动机者获得个人信息后进行骚扰、跟踪甚至直接侵害用户权益[22]。具有侵略性的黑客行为一旦击破网络公司保管个人信息的安全壁垒，必然导致大量个人信息泄露，进而产生诸如利用用户的个人信息进行身份欺诈或财务欺诈等严重事件。例如，美国消费者信用报告机构 Equifax 遭到黑客攻击，导致 1.455 亿个社会安全号码、以及仍在有效期内的 20 多万个信用卡号码和大约 18.2 万份政府签发的身份证明文件（如驾照、纳税人身份证件、护照和军人证等）被泄露。

三、《个人信息保护法》的规范效果

域外立法，如欧盟《通用数据保护条例》与美

国《加利福尼亚州消费者隐私法》是有关个人信息保护法律的代表，对我国个人信息保护立法具有借鉴作用。《民法典》第1035条规定“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”，并确立公民对其个人信息享有同意权（第1035条第1款）、查阅权（第1037条第1款）、更正权（第1037条第1款）、删除权（第1037条第2款）等权利。《个人信息保护法》更是对管辖范围、处理要求等具体内容进行明确，强调个人信息主体所享有的丰富权利，以遏制日益严重的不当收集与错误使用个人信息的行为。

㈠ 《个人信息保护法》的相关规定

《个人信息保护法》包含公法与私法规范，旨在保护当今在数据驱动的网络世界中公民个人信息权益不受侵害，尤其增加了跨境管辖范围规定与数据处理要求规定，授予个人信息主体查阅、更正、删除等权利，并要求个人信息处理者采用风险评估措施等。《个人信息保护法》是保护个人信息的基本立法，通过制定个人信息保护的基本原则和制度并同时在实体规范与程序规范两个层面予以明确，以创立个人信息保护的法律完备体系[23]。

1. 对个人信息主体知情同意的规定。《个人信息保护法》第13条第一项规定处理个人信息应“取得个人的同意”，第14条规定“基于个人处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。……个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意”，法律要求处理个人信息的同意应当由信息主体在充分知情的前提下作出，体现对个人意思自治的保护。同时，第15条还对同意要求进行补充规定，即“基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力”。需要注意的是，这里相对于《个人信息保护法（草案一审稿）》增加了“个人信息处理者应当提供便捷的撤回同意的方式”以及第2款规定的“不影响撤回前基于个人同意已进行的个人信息处理活动的效力”。

2. 对个人信息处理者通知义务的规定。《个人信息保护法》第14条规定的个人应在充分知情的前提下作出同意体现了对个人信息处理者的督促作用，只有网络公司等个人信息处理者履行了适当的通知说明义务，个人才能够充分知情。第17条规定“个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项”，包括“名称或者姓名、联系方式、处理目的、处理方式”等，第18条规定除非依法律规定需要进行保密或无需告知情形下才可以不进行说明。此外，《个人信息保护法》第24条第3款规定“通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定”，这里的“自动化决策方式”主要指个人信息处理者依据计算机算法对用户数据在先分析后作出的决策，例如网络打车软件的动态定价协议等。

3. 对个人信息匿名化的规定。《个人信息保护法》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，不包括匿名化处理后的信息”，这里将匿名化处理的个人信息从法律保护范围中排除。立法机构认为，匿名化处理的个人信息无法指向特定个人，即使被其他方式使用也不会对个人产生不利影响，如《个人信息保护法》第73条第四项进行的说明，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”。

㈡ 处理现实问题的困境

《个人信息保护法》保护网络用户等个人信息主体的各项权益，兼具规范与促进网络公司适当的处理行为。但是，若仅按目前条文的规定对网络公司的信息处理行为进行监管，虽能够起到一定的规范作用，但仍然存在保护困境，无法实现网络空间用户知情同意与解决网络公司不正当处理个人信息的问题。

1. 用户选择同意权利的“名存实亡”。《个人信息保护法》授予用户知情同意权、撤回权、查阅复制权、更正补充权、删除权、解释说明权等权利，这些权利得以行使的前提是用户拥有独立自主的缔约地位，若用户依附于网络公司，则缔约时网络公司完全可以利用服务协议或隐私政策对前述权利进行排除或要求用户“主动放弃”。虽然《个人信息保护法》规定个人信息处理者应当以明白易懂的方式向用户发出同意请求，且用户作出同意表示应在完全自愿的情形下，然而这种理想模式在现实操作中难以实现。鉴于网络公司缺乏有效通知等愈演愈烈的不正当信息处理行为，导致用户无法自由地、知情地订立协议。更为严重的是，如果用户决定退出个人信息的处理过程，就拒绝了或无法使用网络公司提供的各项服务。《个人信息保护法》第

16条规定“个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由，拒绝提供产品或者服务”，似乎赋予用户拒绝网络公司处理个人信息但同时可以继续使用网络产品或服务的权利，但该法条后半句规定“处理个人信息属于提供产品或者服务所必需的除外”，这里实际上给予网络公司一个“很好的理由”继续收集、使用、加工个人信息。何为提供产品或服务所必需处理的个人信息并没有法律的明确规定或行业内的一致意见，完全在于具体场景中网络公司单方面的决定，《个人信息保护法》第16条所欲构建的个人拒绝权利的实际意义并不明显。[24]“用户选择退出”本质上意味着退出整个互联网行业所提供的相同或类似的产品与服务，原因在于大多数网络公司都采取同样的做法与条款设计，用户只有在同意的前提下才被允许访问网站与使用产品。社会的不断发展使单位、学校、公寓、餐厅、车站等个人活动的所有场所都更加依赖于互联网，而作为个体的用户无法承受退出体系化网络服务的代价，用户只能被动地接受网络公司的信息处理方案。因此，根据《个人信息保护法》目前的规定，虽然表面上构建出个人信息主体与个人信息处理者之间的平等协商机制，实质上网络公司仍然可以自由地收集大量个人信息。

在“隐私自我管理”的框架下，法律为人们提供一套权利，使他们能决定如何管理自己的数据，创造一种保护个人信息的错觉，然而在现实中，这些权利是毫无意义的。对于同意收集、披露和使用个人信息的成本和收益，用户缺乏作出知情、理性选择的能力。有学者认为，“寻求个人信息的压力无处不在，它们发生的情况多种多样，似乎又没有其他选择，而所有这些因素共同造成了一种抵制是无用的感觉”[25]，“个人时间、资源贫乏，且缺乏必要的专业知识，无法有意义地利用这些个人权利”[26]，“只要公众把个人信息保护理解为个人‘自己决定何时、采用何种方式以及在何种程度上与他人分享有关自己的信息’的权利，就不会有很好的监管形式”[27]。这些观点说明了用户在网络空间中的自主性较弱，完全依赖当事人之间所谓平等协商的服务协议或经用户同意方能生效的隐私政策并不能防止网络公司对用户个人信息的滥用和侵害。

《个人信息保护法》规定知情同意规则，网络公司也将提升服务协议与隐私政策的可读性以及更为用户考虑的改变，但要实现用户与网络公司针对个人信息条款的同一理解水平并不可能。用户难以在短时间内完全理解网络公司的个人信息处理规则，而基于“要么接受要么放弃”的行业一致做法，即使用户理解个人信息处理规则也不能针对实质不平等条款进行有力对抗，“当用户发现自己一开始就没有选择条款的权利时，他们为什么要阅读服务条款？其无法获得网络公司的回应，也不能就隐私政策进行谈判”。[28]《个人信息保护法》的规定并不能实现用户准确理解与自愿同意协议内容，虽然个人信息保护立法对网络公司的错误行为进行纠正，但用户选择同意权利的“名存实亡”无法为其在网络空间的活动中提供更强的信任感。

2. 匿名化及其逆过程对个人信息权益的侵害。完美的个人信息匿名化在网络空间中无法实现，当大数据高度集合时便可以很容易地重新识别信息主体与相关信息。例如，美国政府机构“集体保险委员会”（Group Insurance Commission，GIC）向研究人员免费提供删除了姓名、地址、社会保险号和其他“显著标识符”的马萨诸塞州政府雇员的匿名化就诊记录，时任州长威廉·维尔德（William Weld）向公众保证，GIC删除了就诊记录的显著标识符，对患者隐私进行绝对保护。然而，研究生斯威尼（Sweeney）仅根据未删除的邮政编码、出生日期和性别这三个属性就很快找到了州长的就诊记录。[29]可见，匿名化的逆过程或称之为去匿名化能根据仅有的少量信息找到匿名化个人信息的原主体。

《个人信息保护法》第4条与第73条涉及对匿名化个人信息的规定，相较于《个人信息保护法(草案一审稿)》第24条第2款规定的“个人信息处理者向第三方提供匿名化信息的，第三方不得利用技术等手段重新识别个人身份”而言，更不利于对用户个人信息权益进行保护。网络公司为了精准营销等目的而重新识别用户个人信息存在强大的经济动机，特别是技术进步以及更大利益诱惑使得新的针对各种匿名化信息进行的处理方式成为可能。例如，数据分析公司对各种个人信息进行收集和分析，特别是使用自动算法与自动比对软件对所收集的匿名化信息进行处理，并且通过去匿名化方法找到这些个人信息背后的主体，以便推送针对性广告。随着匿名化信息的重新识别成为一项可行且有利可图的业务，去匿名化风险必然增加，用户个人信息权益也将受到越来越多的侵害。

在我国实践中，网络公司等个人信息处理者对个人信息的不正当处理行为一部分源自于对个人信息的直接处理，即对于尚未匿名化的个人信息进行

非法使用以获得超额利益，针对此问题《个人信息保护法》已经制定事前防范与事后处罚条文，赋予信息主体范围更广的知情权、拒绝权等主动权利。而另一部分则来源于对匿名化信息进行去匿名化操作，对网络用户的生活安宁进行侵扰甚至侵害各项隐私权益，此时需要重新设计与优化个人信息的匿名化措施。

四、通知义务完善与动态的匿名化

《民法典》第1038条第1款规定，“信息处理者不得泄露或者篡改其收集、存储的个人信息；未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外”。该条文与《个人信息保护法》第4条第1款存在相似的问题，在网络技术快速发展促使去匿名化越来越可行的背景下，“经过加工无法识别”的个人信息概念已经难以成立，即使存在无法识别的个人信息，当切断其与信息主体的所有联系时，所具有的数据价值也将消灭[30]。《个人信息保护法》的实施旨在对于网络空间中普遍存在的缺乏通知、滥用用户个人信息等不正当的信息处理行为进行全面规制，以及在对个人信息进行保护时不影响其使用价值及促进互联网行业的发展。但是，立法上的设计对于网络空间中普遍存在的现实问题并不能发挥个人信息保护与促进行业发展的平衡作用，用户难以依据法律规定对个人信息进行有效控制，也不能获得有意义的选择权利。

解决网络空间用户知情同意的虚化与网络公司不正当处理个人信息两大困境的可行途径是在完善通知义务的同时设置更为严格的动态匿名化方法，要求网络公司进行充分通知有利于用户在知情的情形下作出真实同意的意思表示，从而抵制网络公司滥用个人信息的行为以及可能产生的安全风险，而利用严格的动态匿名化方法将防止不完全匿名化个人信息的使用行为对信息主体造成的损害。

（一）通知义务的完善

纸质合同中，法律要求条款提供方履行适当的通知说明义务，并就关涉权利义务的重要格式条款进行足以引起对方注意的文字、字体、符号或者其他明显标志的提示。而在用户与网络公司订立的服务协议等网络合同中，用户处于更为劣势的缔约地位，对于网页中存在的各种陷阱缺乏敏感性，且对于后台运行程序等网络技术完全陌生，加之对使用网络产品或服务的迫切心态及有限理性，导致在不知情或不理解的情况下对网络公司提供的协议内容表示同意。因此，法律在对网络公司等个人信息处理者的通知义务进行规定时，应当考虑网络合同场景与纸质合同场景的不同，更加关注用户的感知。

1. 条款内容的显著通知。纸质合同中，条款字体的大小和位置与合理通知义务的履行具有相关性，网络服务协议也应考虑这些因素，且作出更多努力以获得用户的实际同意。考虑到网络活动多以视觉为导向，网络公司在进行充分解释说明时应增加图片来提醒用户阅读服务协议。例如，纸质合同中的条款为“通过下订单，您将同意我们收集您的个人信息”，而在网络服务协议中，条款内容应扩充为“通过下订单，您将同意我们收集您的姓名、地址、联系电话等个人信息以及其他信息，其中包含浏览踪迹、购买清单、信用卡信息等”，且增加内容“点击此处获取更多信息”以提示用户重要条款，并附上“粗体感叹号”等警示图片。而且，基于网络环境的特殊性，网络公司应尽量保障用户专注于阅读条款内容而不是让用户阅读条款的同时利用网络交易流程的其他活动分散其注意力。例如，脸书公司网页上权利义务条款的超链接放置在“立即注册”字段下方，将大的绿色“注册框”与字体小得多的格式条款、数据使用说明、Cookies协议等内容放在一起，诱使用户忽略繁杂的个人信息条款内容而直接点击“注册”按钮[31]。作为条款起草方，脸书公司应该将协议条款设置的更为显著，包含更多的提示信息，例如可以在“提供免费服务”条款旁边附加内容——“我们提供免费服务，但是我们将无偿使用您的个人信息，请阅读您和脸书公司之间具有法律约束力的协议条款”。

2. 重要事项的单独通知。网络公司应该进行充分通知使用户阅读服务协议的内容而不是仅仅看到服务协议的提出方式。例如，可以要求网络公司在同一协议中就不同事项进行分别通知，且只有在用户就每一重要事项表达同意后才能生效，以构建特定的同意许可。亚马逊公司（Amazon）为了详细说明需要用户授权的内容和可能承担的责任，要求作为非起草方的用户在每一个承诺的重要事项之后点击同意[32]。这种多重形式的通知要求具有进步意义，可以有效地避免用户一次点击行为导致的概括同意、而实际上并未阅读或理解授权内容的“无意视盲”的结果的出现[33]。当网络公司从用户处获得较多个人信息时，应该与用户进行多轮谈判，而不是用户的一次点击行为就能够使网络公司获得所有信息。也就是说，若网络公司寻求从用户处获得更多

的权利作为交互的一部分，如收集用户个人信息以实现多个营销目的或广泛的使用用户生成内容，应提供比不索取或很少索取对方授权更加繁重的缔约过程。虽然适用多重点击行为取代一次点击行为确实会增加用户的行为负担，但是这种多重点击形式将引入订立协议的事务障碍，有利于表明条款内容的重要性。而且，在追求更高效率与更快速度的网络活动中，对协议内每一重要事项的点击同意行为并不要求用户付出太多时间，与一次点击行为所花费的时间仍在同一数量级内，具有可行性。

（二）动态的匿名化方法

信息的自由流动有助于实现许多重要的政治和经济功能，正如艾拉·鲁宾斯坦（Ira S. Rubinstein）和伍德罗·哈佐格（Woodrow Hartzog）所说的，“对信息收集和披露的全面和强有力的禁止将使组织和整个社会付出难以置信的代价。”[34]匿名化的目的是将这些数据点关系与可以收集到的关于特定个人及其身份的信息知识脱钩，使信息的自由流动无法对信息主体造成困扰。然而，随着匿名化作为个人信息及隐私保护的弱点暴露出来，其实现平衡的能力受到质疑。由于数据隐私和数据效用之间存在负相关关系，定义适当的平衡成为关于匿名化是否足以保护用户个人信息辩论的核心。有学者认为，匿名化具有减少数据共享机会成本的明显优势。[35]也有学者建议放弃对匿名化的依赖，认为完全放开对匿名化数据的监管所带来的效益并不能多于解决纠纷的成本。[36]本文提出更为严格的动态匿名化方法，使匿名化在保护个人信息与促进数据价值实现的平衡功能得以体现。匿名化不应被当作一次性操作，应针对已经使用的匿名化信息进行定期风险评估，包括对可能风险与实际损害的分析，当可能风险较高时，此时要求个人信息处理者强化处理程序，防止对信息主体的损害，当已经产生实际损害时，则必须进行重新匿名化。动态的匿名化方法是基于风险、损害分析的匿名化方法，通过仔细评估数据环境并采取预防措施来管理风险。

1. 对可能风险的分析。对可能风险的分析是指，法律上对匿名化信息的风险定义不仅基于对现实情形的个案评估，而且基于特定情况下对任何给定匿名化信息被重新识别的潜在风险评估。分析可能风险意味着应定期评估与去匿名化有关的风险，包括匿名化信息被重新识别的可能性及产生损害的可能性。当匿名化信息存在去匿名化可能或对该信息的处理行为可能对信息主体造成损害时，其程序性规定需更为严格，如要求网络公司提供更为详实和可行的信息保护措施、风险评估报告、紧急应对方案等。严格的程序性要求对去匿名化个人信息的可能性和损害程度进行预先评估，并根据评估结果进行矫正，风险越高，程序性措施就越严格。

2. 对实际损害的分析。对实际损害的分析侧重于评估不充分匿名化所带来的特定个人信息及隐私的损害，并根据这种损害的检测及时发现网络公司的去匿名化企图。也就是说，只要匿名化信息的处理行为仍会造成损害的，则不能认定为完全匿名化，需要根据具体的使用情况进行再匿名化处理。但是，这种措施也遇到困难，因为它依赖于将法律上可认定损害的因果关系追溯到匿名化过程中，而因果关系的认定在侵权法体系中本身就是一个复杂的过程，如冯·巴尔所说，“因果关系就是侵权法要求的必要联系，……对于何为必要的联系，是没有普遍适用的答案的”[37]。为了保护用户个人信息权益不因个人信息的泄露而遭受损害及由于网络环境的开放性与瞬时性等特征造成的损害无限扩大，应在确定匿名化信息的不当使用与用户损害具有相当因果关系时，即认定个人信息匿名化不完全并进行再匿名化处理。

根据匿名化信息的可能风险与实际损害的分析，匿名化信息与不完全匿名化个人信息之间的界限是不固定的，并随着时间的推移而演变。例如，在某个时期内现有技术无法将匿名化信息进行去匿名化处理，则此时的信息可任意使用，但是当某一技术的出现能够对前项匿名化信息进行去匿名化时，则应进行再匿名化处理，此时未进行再匿名化处理的匿名化信息不属于可任意使用范畴。动态的匿名化方法强化对用户个人信息的保护，可防止不完全匿名化及去匿名化操作对用户权益造成损害。

五、结论

就网络用户同意表示的非真实性与网络公司处理行为的不正当性等个人信息保护问题而言，《个人信息保护法》的相关规定更像是为用户提供自我管理框架，其必须主动维护并主张自己的权利，而用户在缺乏同意收集、使用、披露个人信息的成本和收益方面作出自由、知情、理性选择能力的前提下，网络公司获得用户同意的处理个人信息行为实际上是基于其不平等的缔约地位，且不断增加的不正当处理行为将对网络用户权益造成更多损害。较为可行的方法是增加网络公司通知义务的规定以及设立更为严格的动态匿名化方法，使对网络空间个

人信息处理行为的规制从过时的自我管理模式向考虑现实的现代方法转变，这不仅有利于用户作出更加独立自主的真实意思表示，而且也发挥了法律在保障个人信息数据价值的同时保证用户权益不受侵害的平衡作用。

注释：

①⑫ Katherine J. Strandburg, Free Fall: The Online Market's Consumer Preference Disconnect, University of Chicago Legal Forum, 2013, 95, p.150.

② 参见上海艾瑞市场咨询有限公司专题资料汇编：《艾瑞咨询系列研究报告》2018 年第 8 期。

③ Daniel Susser, Beate Roessler, Online Manipulation: Hidden Influences in a Digital World, Georgetown Law Technology Review, 2019, 4, p.1.

④ 申卫星：《论数据用益权》，《中国社会科学》2020 年第 11 期。

⑤ 刘权：《论网络平台的数据报送义务》，《当代法学》2019 年第 5 期。

⑥ 王叶刚：《论网络隐私政策的效力——以个人信息保护为中心》，《比较法研究》2020 年第 1 期。

⑦ 例如，《大众点评用户服务条款》规定："本条款为《美团点评平台用户服务协议》（包括但不限于所附的《美团点评平台隐私政策》）的必要组成部分。《美团点评平台用户服务协议》将同时适用于大众点评的各项服务。如本条款与《美团点评平台用户服务协议》文本内容存在冲突之处，则以时间上最新发布的内容为准，发布时间相同的，以本条款为准。本条款有待明确、存在歧义或未规定之处均以《美团点评平台用户服务协议》中的规定为准。"

⑧ 王利明：《合同法研究》第 1 卷，中国人民大学出版社 2011 年版，第 545—549 页。

⑨ James P. Nehf, Recognizing the Societal Value in Information Privacy, Washington Law Review, 2003, 78, pp.1–28.

⑩ Robert A. Hillman, Jeffrey J. Rachlinski, Standard–Form Contracting in the Electronic Age, New York University Law Review, 2002, 77, pp.438–439.

⑪ 参见刘红亮：《网络市场垄断行为发展趋势及危害研究》，《中国市场监管报》2017 年 3 月 14 日。

⑬ Cass R. Sunstein, Bounded Rational Borrowing, University of Chicago Law Review, 2006, 73, pp.249–252.

⑭ 参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，《政治与法律》2016 年第 7 期。

⑮㉕ Richard Warner, Robert Sloan, Beyond Notice and Choice: Privacy, Norms, and Consent, Suffolk University Journal High Technology Law, 2013, 14, pp.370–390, p.370.

⑯ 参见马更新：《平台经营者"相应的责任"认定标准及具体化——对电子商务法第 38 条第 2 款的分析》，《东方法学》2021 年第 2 期。

⑰ 北京市海淀区人民法院（2018）京 0108 民初 13661 号民事判决书。

⑱ 南京市鼓楼区人民法院（2013）鼓民初字第 3031 号民事判决书。

⑲ 江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

⑳ 根据皮尤研究中心（Pew Research Center）的研究数据显示，"大约三分之二（68%）的互联网用户不赞成搜索引擎和网站跟踪他们的在线行为，以定向投放广告"。参见 Russell Heimlich, Internet Users Don't like Targeted Ads, Pew Res. Ctr. 2012, Mar.13.

㉑ 程啸：《民法典编纂视野下的个人信息保护》，《中国法学》2019 年第 4 期。

㉒ Julie Cohen, What Privacy is For, Harvard Law Review, 2013, 126, pp.1904–1915.

㉓ 周汉华：《个人信息保护的法律定位》，《法商研究》2020 年第 3 期。

㉔ 例如，脸书、照片墙（Instagram）、优步等一些受欢迎的网络产品都要求用户同意其用户协议及隐私政策，否则将无法使用网络服务。

㉖ Lilian Edwards, Michael Veale, Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For, Duke Law & Technology Review, 2017, 67, pp.16–18.

㉗ Lauren E. Willis, Why Not Privacy by Default? Berkeley Technology Law Journal, 2014, 133, pp.29–61.

㉘ How Silicon Valley Puts the "Con" in Consent, New York Times, Feb. 2, 2019.

㉙ Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, UCLA Law Review, 2010, 57, pp.1719–1720.

㉚ 刘颖、谷佳琪：《个人信息去身份化及其制度构建》，《学术研究》2020 年第 12 期。

㉛㉜ Nancy S. Kim, Wrap Contracts: Foundations and Ramifications, Oxford University Press, 2013, p.203.

㉝ Christopher Chabris, Daniel Simons, The Invisible Gorilla: And Other Ways Our Intuitions Deceive Us, Crown, 2010, pp.6–7.

㉞㊱ Ira Rubinstein, Woodrow Hartzog, Anonymization and Risk, Washington Law Review, 2016, 91, p.731, p.739.

㉟ Jane Yakowitz, Tragedy of the Data Commons, Harvard Journal of Law & Technology, 2011, 25, pp.1–4.

㊲ 程啸：《侵权责任法》，法律出版社 2021 年版，第 235—236 页。

作者简介：夏庆锋，安徽大学法学院副教授，安徽合肥，230039。

（责任编辑　李　涛）