

# 透明化生存中的自主性构建： 算法推荐的隐私问题与规制路径

杜永欣<sup>1</sup>，周茂君<sup>2</sup>

(1. 北京大学新闻与传播学院，北京 100871；2. 武汉大学新闻与传播学院，湖北武汉 430072)

**摘要：**个人信息与隐私保护是当前互联网与信息安全治理领域的紧迫性议题。在信息要素成为基础资源的数字化社会，基于个人信息挖掘与利用的算法推荐模式成为当前实现精准传播的创新路径，而如何权衡个人信息商业化利用和信息隐私保护之间的冲突，是算法全面嵌入社会语境下技术风险应对的时代命题。随着信息公私领域的消解，隐私边界变得模糊而难以界定，隐私信息的多元属性日趋凸显，加之信息资源的不对等，常态化的信息流动极大增加了个人隐私风险。当前，以“识别性”为核心的个人信息范围界定和诉诸“授权同意”的隐私保护机制面临现实困境，全面的数字化建构使得个人信息自主性趋于消解，透明化生存中个人信息自主与隐私自控难以实现。以信息赋权推进个人信息自主性的构建，有赖于实现差异化场景中的信息分类与风险分级，以技术赋能行业自律与隐私管理，进而形成法律规制与自治协同的规范体系。

**关键词：**算法推荐；隐私保护；信息赋权；信息安全；自主性

**中图分类号：**G206

**文献标识码：**A

**文章编号：**2096-8418 (2022) 06-0010-10

## 一、问题的提出

在信息技术发展日新月异的数字时代，信息资源作为社会运行的“原料”，已成为商业竞争中不可或缺的关键要素。随着数据信息在行业发展中的价值日益凸显，个人信息<sup>①</sup>获取与利用成为网络服务平台提升经济效益、获得竞争优势的有效途径。当前网络行为追踪、智能推荐算法等技术的应用，使得大规模的信息获取、储存和分析成为可能，技术的全面渗透为用户网络行为处理提供了前所未有的可量化维度。在一切网络行为都可被记录的数字化社会，数据洪流所引发的信息安全隐患和隐私风险与日俱增。

随着信息商业化应用进程加快，基于个人信息采集和利用的算法推荐服务模式，为网络服务提供者带来了可观收益。然而频繁出现的数据信息泄露事件也引发了普遍的隐私担忧，借由网络服务对于个人敏感信息的操控更是不断挑战隐私“红线”，数字时代的个人信息与隐私保护呼声日益高涨。早在2016年，《中国个人信息安全和隐私保护报告》<sup>②</sup>公布的一项针对全国范围的100多万份问卷调查结果中，就有超七成的受访者认为个人信息泄露问题严重，因网页搜索、浏览等泄露个人信息，而遭受广告持续侵扰的比例达53%，其中60%的受访者不知如何维权。鉴于数字时代个人信息与隐私保护问题

**作者简介：**杜永欣，女，博士研究生；周茂君，男，教授，博士生导师。

<sup>①</sup> 个人信息、个人隐私、个人数据是当前较常混用的概念，美国习惯使用“个人隐私”，如1974年颁布的《隐私法案》(Privacy Act of 1974)；欧盟多使用“个人数据”，如最新颁布的《通用数据保护条例》(GDPR)；我国多采用“个人信息”的概念，如《个人信息保护法》，并且在学术研究中也多采用“个人信息”保护的概念讨论隐私问题，本文亦采用这一概念框架探讨个人隐私问题。

<sup>②</sup> 参见互联网法治研究中心：中国个人信息安全和隐私保护报告。http://www.199it.com/archives/540836.html。

愈发紧迫, 研究者们从法律保护、技术保护、行业自律以及自我防范四大方面, 探讨了如何应对日益严峻的隐私危机,<sup>[1][2]</sup> 其中以行业自律为主导的美国模式, 以及诉诸严苛法律保护的欧盟模式, 在保护个人信息及隐私领域具有广泛影响力。随着世界范围内个人信息保护立法潮流的兴起, 2018 年欧洲《通用数据保护条例》(General Data Protection Regulation, 简称 GDPR)、2020 年《加利福尼亚州消费者隐私保护法案》(California Consumer Privacy Act, 简称 CCPA) 相继实施, 旨在进一步规范互联网时代迅速发展的个人信息收集和使用行为。在我国, 2012 年全国人大常委会通过《关于加强网络信息保护的決定》, 开启了我国个人信息保护的立法之路, 此后我国关于个人信息保护的规定在《网络安全法》《消费者权益保护法》等法律法规中有所体现, 至 2021 年《个人信息保护法》出台, 以及 2022 年 3 月国家网信办等四部门联合发布的《互联网信息服务算法推荐管理规定》正式施行, 网络信息安全和隐私保护在国家层面的法律制度保护规范逐渐确立并日益完善。

依托大数据与智能算法提供精准推荐的网络服务模式, 其核心逻辑在于深度的个人信息挖掘与定制化的信息需求满足, 由此也必然面临个人信息商业化利用与信息隐私保护之间的权衡问题。例如当前几乎无处不在的精准推荐广告, 网络服务提供者能够通过实时数据获取, 精准定位目标用户及其需求特征, 以有效提升广告传播效果;<sup>[3]</sup> 但随着个人隐私保护意识的增强, 网络服务提供者的信息操控行为一旦被用户感知, 则往往会触发个人隐私规避心理, 从而对精准推荐内容产生“抗拒”, 传播效果也将大打折扣,<sup>[3][4]</sup> 隐私关注成为用户网络行为与传播效果研究的重要影响因素。<sup>[5]</sup> 然而, 倘若对个人信息收集和使用加以限制, 则可能导致广告效果下降,<sup>[6]</sup> 缺乏针对性的广告不仅难以奏效, 而且容易造成广告侵扰。另外, 信息规范与算法规制体系的构建, 也面临相应的监管成本增加问题, 同时也可能阻碍网络服务平台的数据驱动发展能力, 增加其运行成本, 从而影响企业创新发展的方向。<sup>[7][8]</sup> 因此, 如何有效应对由个人信息商业化利用而引发的信息权益冲突, 是算法推荐模式持续发展而亟待解决的问题。如今智能算法技术已深度嵌入数字化社会, 个人信息是算法推荐不可或缺的数据基础, 而隐私问题更是触及算法推荐逻辑的核心, 信息权益的合理权衡成为技术风险应对的重要命题。新时期我国对个人信息与隐私的保护进入精细化发展阶段。鉴于该问题涉及多元主体以及多方利益关系博弈, 探讨算法推荐中的个人信息与隐私问题, 有助于进一步厘清技术变革背景下个人信息商业化利用过程中所蕴含的风险, 进而寻求应对个人信息与隐私危机的有效路径。这对于推进算法推荐模式的规范发展乃至信息安全领域治理体系的完善具有重要意义。

## 二、冲击与再诠释: 个人信息流动中的隐私风险

信息与隐私密不可分。《论隐私权》一书提出了“隐私权”概念, 其强调个人免受打扰的“独处权”, 来源于不受侵犯的人格权范畴。<sup>[9]</sup> 桑德拉·佩特罗尼奥将“隐私边界”视为人们管理公共领域与私人领域的界限, 认为它并不是固定的, 而是可渗透和可伸缩的。<sup>[10]</sup> 随着媒介技术的变革发展, 信息的收集、传播、利用和交换方式也发生改变, 传统时期界限分明的隐私观, 逐渐转向数字化社会以个人信息自控为核心的隐私内涵, 普遍的信息流动也导致了前所未有的隐私风险。

### (一) 缘起: 信息公私领域的消解与隐私边界的解构

任何一种新技术的出现, 往往伴随着人们生存与生活方式的变迁。信息技术对隐私保护的冲击, 首先表现为大量的个人网络行为被持续地记录、保存和利用, 私人领域逐渐向公共领域延伸, 公共领域不断向私人领域渗透, 二者的界限日益模糊, 由此隐私边界渐趋消融。在早期以“场所”为导向的隐私界定中, “公共”和“隐私”被视为天然对立的观念, “公共”则意味着公开, 非私密空间不存在任何隐私。<sup>[11]</sup> 正如阿伦特所说, 任何在公共场合所见、所闻的东西, 都有最大程度的公开性。<sup>[12]</sup> “公共场所无隐私”的主张也一度成为法律实践中的隐私判定标准。然而在以数据为基础、由算法建构的数

字化社会,一方面,人们的社交活动实现了以“圈子”为核心向以“关系”为纽带的网络交往转向,个人信息范围逐渐向外延伸,信息的公私边界渐趋消融;<sup>[13]</sup>另一方面,媒介技术的变革极大增强了“万物皆可追踪”的可能性和海量数据长期储存的便利性,这使得用户成为被数据化、符号化的透明个体。个人信息被广泛用于信息的精准匹配与传播效果达成的目的,这意味着私人信息也成为可以被开发利用的“公共资源”。例如无论是具有公共属性的网站搜索、留言评论行为,还是在私人网络空间进行的朋友聊天、动态发布、好友互动与分享等,都能以数据的形式加以留存和使用。网络虚拟世界与现实生活密切交织,信息流动与共享使得公共领域与私人领域的边界变得模糊而难以区分,以往被视为私人领域的个人信息,如今也以“数字记忆”的方式进入公共空间。因此,数字化社会的个人信息正被赋予更多的公开性和公共属性,用户对其不愿公开的私密信息逐渐失去控制,作为私人领域“不受干扰”的私域空间正逐渐消失。

## (二) 冲突:个人信息属性的多元化与隐私内涵的嬗变

在传统的隐私观念范畴,隐私所代表的私密性是与公共空间所具有的公开性相区分的概念,隐私内涵的相对性决定了其通常是社会主体间利益协商的结果,基于不同时期社会公共利益的考量,对于隐私保护难免有所取舍。传统时期个人信息的核心功能在于可交流属性,它是个体参与社会生活用以标识自身的工具,<sup>[14]</sup>客观上难以通过共享个人信息来获取经济利益。由于隐私权代表着人格权范畴的合法权利,其强调个体自由与个人尊严的不容侵犯性,这意味着私人信息的商业化利用是不被允许的。数字时代个人信息呈现出普遍的流动性特征,技术赋能使得个人信息的商业价值得以充分挖掘,由此也引发了隐私内涵的嬗变。信息的流动与交换所创造的价值增益是数字经济发展的根本动因,数据成为蕴含巨大商业价值的社会资源,而技术变革则为个人信息获取和使用提供了手段。在商业逻辑的助推下,作为隐私的个人信息逐渐从人格权中剥离,并能够加以商业化利用,由此个人信息的交换价值和商品属性得以充分发掘,其财产价值逐渐显现。在大数据与人工智能技术应用日益成熟的背景下,个人信息也被推至商业化应用与增值的快车道,其中算法推荐广告行业集中体现了个人信息的商业化利用过程。以实时竞价(Real Time Bidding)广告为例,数据分析与需求匹配是精准投放的关键,实际上在整个广告投放流程中,个人信息在各类数据处理和广告交易平台上为网络服务提供者所利用和消费。<sup>[15]</sup>尽管个人信息关乎人格尊严,但现实中又具有可交易的财产性特征,<sup>[14]</sup>数字化社会频繁出现的隐私争议,究其原因,也主要在于个人信息与隐私的保护和利用冲突。一方面,在这场以个人信息价值挖掘为核心的交易活动中,网络服务提供者能够通过新技术手段深入洞察用户网络行为特征,依据其所获得的个人信息进行内容推荐决策,以满足用户个性化的信息需求,信息传播的运行效率得以极大提升,并且服务双方都在一定程度上有所增益。而就个人信息与隐私保护而言,当用户网络行为信息成为网络服务提供者理解和满足用户需求的基础,更多具有敏感性的私人信息也流向了公共空间,隐私信息不再是人格权范畴完全不容侵犯的领域,而成为能在合理预期范围之内进行流转的“商品”。信息隐私的这种“流动”状态下的财产属性,也在一定程度引发了用户在人格权益层面的让渡或受损风险。

## (三) 失衡:信息资源不对称加剧隐私保护冲击

信息技术的发展为更高效地释放个人信息价值提供了可能。鉴于网络服务提供者与用户个体之间所掌握的信息资源差异悬殊,这种信息持有的不对称也导致了信息价值收益的失衡。首先,数字化社会由网络平台主导的信息流动模式,从根本上颠覆了传统时期以个人为导向的信息分享机制,网络服务提供者成为个人信息的持有者和使用者,用户则成为被算法“操控”的对象,个人信息权益越来越难以保障。借助于各种数据追踪技术,网络服务提供者能够源源不断地获取用户网络行为信息,从而形成无形的“监控”网络,通过数据资源与算法程序的结合,网络服务提供者能够将所获得的个人信



息充分用于提升自身效益和市场竞争能力,而用户则逐渐沦为网络服务中被动的信息资源提供者,无法充分享有应有的信息价值收益。另一方面,算法技术的“排他性”也带来了“算法黑箱”问题,即由于算法的不透明性所引发的令人难以理解的状态,<sup>[16]</sup>本质上反映了算法服务的使用者对其中原理以及意图的不知情。由于算法技术作为数据输入、数据处理以及数据输出的一套运作程序系统,普通用户很难明确其中复杂的技术原理,算法的不透明性与不可解释性特征,使得网络服务提供者与用户之间存在着严重的信息不对等,<sup>[17]</sup>前者凭借充分的信息资源持有优势,更容易滋生算法偏见、利益操控等问题。因此,在由网络服务提供方主导的这场资源差距悬殊的“协商”中,双方巨大的“信息鸿沟”使得网络服务提供者占据绝对优势,信息资源持有失衡让用户更容易沦为精准传播中一击即倒的“靶子”。<sup>[15]</sup>数字时代的隐私忧患席卷而来,网络服务提供者通过信息资源占有与价值开发而广泛受益,而用户则在算法黑箱面前无能为力,既无从知晓哪些个人信息被收集,也无法明确个人信息的使用和流向。这种信息不对称助长了算法推荐中网络服务双方权利不平等局面,用户的弱势地位造成无可避免的隐私让渡,隐私顾虑冲击着网络服务双方的信任机制,由此难以建立持续而良好的协作沟通关系。

### 三、算法推荐中的个人信息与隐私保护困境

隐私意味着自我与他人之间的界限,是自我意识发展的前提,“没有一定程度的隐私,就不可能有文明的生活”。<sup>[18]</sup>隐私权的保护旨在使得个人有所隐藏、保留和独处,得为自主而拥有一定范围的内在自我。<sup>[19]</sup>数字化社会的算法建构无处不在,我们犹如身处透明化的社会环境之中,个人隐私却无处遁形。由媒介技术变革所引发的隐私风险,核心在于人们无法有效控制个人信息的流动范围,且信息自控和自决受到算法逻辑的冲击,而当前无论是法律规约还是自律规范,都难以在个人信息的普遍商业化应用中提供有效的信息与隐私安全保障,个人信息自主性正受到全面数字化建构的侵蚀。

#### (一) 法律规制中个人信息识别要素的变迁

个人信息是一切可以识别本人的信息的总和,其中“识别”是构成个人信息的实质要素,包括直接识别和间接识别的信息。<sup>[20]</sup>个人信息的“识别性”是界定个人信息的核心以及信息赋权的基础,<sup>[21]</sup>目前已成为世界多数国家制定个人信息或隐私保护法所采用的个人信息范围界定依据。<sup>[22]</sup>例如欧盟1995年《数据保护指令》、我国2021年实施的《个人信息保护法》,都将“与已识别或可识别的自然人有关的任何信息”界定为个人信息范畴。在实际的隐私纠纷案中,如“朱烨诉北京百度网讯科技有限公司隐私权纠纷案”“英国谷歌定向行为广告案”等,能否准确识别具体个人都是重要的判定标准。

伴随着互联网与大数据技术的变革发展,信息的“识别性”边界日益泛化,可识别信息范围趋于模糊而引起诸多争议,技术变迁背景下的个人信息与隐私保护也面临新的挑战。一方面,信息技术的发展引发了关于信息“识别性”的质疑,“可识别”与“不可识别”的信息范围存在相对性,以往不具备识别性的个人信息,随着新技术的应用也极有可能变得能够进行准确识别。例如以往难实现的地理位置、面部表情识别等,如今都能通过技术手段加以精准识别。除此之外,关联性信息因素使得信息识别变得更为复杂,因为即使是初始阶段无法识别的个人信息,借助于数据关联算法仍能够准确识别出个体,“整合型隐私”衍生出更为复杂的隐私问题。<sup>[23]</sup>另一方面,匿名化处理是个人信息“去标识化”所广泛采用的技术保护手段,并且我国相关法律规定也将匿名化处理后的信息排除在个人信息范围之外,但实际上匿名化处理也可能面临失效问题。由于信息“匿名化”主要是将精细化的个人信息进行模糊处理,使得信息在一般情况下难以识别具体个人,从而达到对数据库中具有敏感性的个人信息加以保护的目。然而由于信息技术不断迭代,匿名化处理后的信息也会面临“再识别”风险,通过强大的关联算法、反加密技术等同样能描绘出个体的“数字画像”,匿名化的技术保护效力在实际应用中难以保证。因此,从法律中个人信息识别性的内涵变迁,到技术实践中匿名化、数据加密等

“反识别”方法的保护局限,技术变革不断冲击着基于“识别性”而建立的个人信息权益基础。

## (二) 行业自治中“授权同意”保护机制的失灵

当前网络服务提供者实现精准推荐主要依赖大规模的数据资源与算法分发机制,且对个人信息收集与使用的精细化程度直接影响其收益。算法推荐对用户个性化需求的满足,需要在个人信息挖掘基础上,实现用户行为的精准预测,这个过程需要依赖大规模的原始数据,因此尽可能多地获取大量的个人信息,是促成推荐内容“千人千面”的必然选择。为了避免网络服务提供者肆意进行用户信息收集和使用,“授权同意”机制成为当前法规中信息与隐私保护的普适机制,<sup>[24]</sup>这意味着需要在用户知情的情况下,授权允许网络服务提供者收集和使用必要的个人信息。为此网络服务提供者须以隐私条款的形式公开其信息收集和使用情况,以确保用户知情后根据自身意愿做出合理选择。虽然授权许可机制为个人信息与隐私保护提供了灵活保障,但实际上由于其中存在明显的权利不均衡和话语不对等问题,多数情况下用户既无法实现有效知情,也无法做出遵从其真实意愿的选择决策。

首先,知情是用户同意授权的基础,而网络服务提供者通过隐私声明予以公开承诺的方式,既缺乏详尽说明信息收集的动机,也无法充分告知数据处理及使用的真实情况。用户的授权决策主要依据已发布的隐私条款,而网络服务提供者作为信息收集和持有方,对个人信息的充分获取与价值挖掘关乎其核心利益,拥有更多的个人信息资源即意味着更强的竞争优势,这就导致其既没有限制采集个人信息的动机,也缺乏有效保护隐私信息的内在动力。作为信息价值收益的获益方,网络服务提供者更期待的是用户主动披露更多信息,即便是隐私声明中的保护承诺,通常也只是出于法规限制的考虑,而为了达到“合规”的目的,所以隐私条款要么形式隐蔽难以发觉,要么内容晦涩难懂,用户很难实现有效知情。在多数情况下,用户并不清楚自己的哪些行为被追踪,更不知道哪些信息、什么时候被收集以及怎样被使用,<sup>[25]</sup>技术手段的不断更迭使得网络服务提供者的信息收集和使用变得更加隐蔽且难以察觉,个人信息权益侵犯也往往是在用户“无感”状况下发生的。另一方面,数字时代的信息流动性特征,也决定了网络服务提供者难以实现充分告知,由于用户授权机制所依据的隐私声明是网络服务提供者关于信息收集、处理和使用的事先预判,因而通常只能涵盖常规的信息处理环节,而在个人信息的“下游”处理中,尤其是涉及第三方信息共享和交易时,信息流转中蕴含着难以预判的未知性。除此之外,一些并不敏感的个人信息片段经过有目的排列、组合后,可能成为具有重要商业价值的信息要素,复杂的整合型隐私问题也加剧了隐私保护困难,<sup>[26]</sup>普通用户很难充分了解其中的技术运作原理,因此更无从得知个人信息收集和使用的真实情况。

其次,个人有效同意的核心在于自主选择,而由于网络服务提供者与用户之间的不平等协商,用户授权同意往往是不得已而为之。网络服务提供者收集和使用个人信息需要获得用户授权,主要借助隐私声明的方式予以说明,用户据此做出“同意”或“不同意”的选择。这种协商方式本身建立于双方信息不对称基础之上,处于弱势地位的用户难以明确网络服务提供者自我揭示的保护规则是否合理,只能参与这场“接受或是离开”的游戏。<sup>[27]</sup>部分隐私条款甚至不被重视,且内容往往流于形式,存在语句不通、重复等明显错误。<sup>[28]</sup>由此观之,隐私声明反而沦为网络服务提供者“免于法律责任”的避风港,授权同意机制成为网络服务提供者“合理”获取个人信息、维护自身利益的另类途径。因此,隐私声明中“非同意即离开”的规则实际上所提供的唯一选择就是“同意”。倘若因隐私顾虑而放弃使用某项网络服务,则可能加剧“数字鸿沟”而沦为网络时代的“信息隐民”,所以用户只能参与到这场不平等的个人信息交换机制之中,<sup>[29]</sup>在此情况之下授权保护机制难有实效。

除此之外,“授权同意”机制还面临用户隐私决策成本问题。充分理解各项隐私政策,需要用户投入大量的时间和精力去解读各项晦涩难懂的隐私规定,若内容条款适时更新,则意味着用户需要持续关注隐私条款的变动,才能获得必要的知情信息。但如果因不满隐私政策而选择退出,寻求其他替代

性网络服务时又必然需要新的成本投入。当前过高的隐私管理成本同样限制了用户的自主选择。事实上, 用户授权通常是只是在有限理性或者无意识情况下做出的选择, 诸多限制性因素使得授权同意保护机制面临“失灵”危机。在尚未有效建立相应规范体系的情况下, 算法推荐机制可以说是以个人信息乃至隐私的商业化利用为代价的。

### (三) 全面数字化建构中个人信息自主性的消解

人的自主性建立于自由意志发挥的基础之上, 而在由数据和算法技术打造的透明化生存环境中, 算法推荐在很大程度上限制了用户的真实选择, 个人信息自主性实现的基础正逐渐被算法推荐逻辑所消解。Solove 认为“数据库中的信息通常只是抓住一些刻板印象和非理性行为, 而无法对人们的个性做出细致入微的刻画, 因此难以反映我们的真实生活”。<sup>[30]</sup> 算法推荐机制基于个人信息展开定制化服务, 在此过程中网络服务提供者根据其所获得的用户网络行为信息, 对个体进行数字化建构, 进而理解和预测其需求及偏好, 从而有针对性地推出满足用户需求的信息内容。由此, 差异化个体被建构成为承载各种标签的“数字画像”, 网络服务提供者基于其捕获的碎片化信息, 不断塑造更趋近其预期的“理想角色”, 而用户的自主决策则成为依附于算法程序的异化结果。借助算法程序的信息筛选与需求匹配, 网络服务提供者可以利用其所掌握的数据信息来推动、劝服、影响、甚至限制用户认同,<sup>[31]</sup> 数据驱动下个性化信息内容的精准触达, 实际上是网络服务提供者对个人自主决策的“理想化”塑造, 这种信息过滤和精准推荐往往并非用户真实情况的体现, 而是经由网络服务提供者事先预设的算法逻辑的结果呈现。

网络服务提供者对个人信息的充分占有, 也为其追求自身利益最大化提供了有效途径, 而越是对用户有更加充分的了解, 网络服务提供者就更容易找出能够说服其进行理想化决策的理由, 从而促进网络服务交易达成。例如为追求更好的广告效果和营销收益, 网络服务提供者通过对个人生活习惯及需求动向的长期关注, 预测用户喜好、分析产品购买率、推测产品使用场景, 为其“量身定制”满足其特定需求的产品或服务。<sup>[32]</sup> 另外, 根据用户信息而采用算法推荐技术对用户实施差别定价, “大数据杀熟”行为侵害了用户的合法权益, 也破坏了互联网市场的交易秩序。<sup>[33]</sup> 根据北京消费者协会 2022 年发布的《大数据“杀熟”问题调查报告》<sup>①</sup> 数据, 七成多受访者认为存在大数据“杀熟”现象, 其目的在于获取更多的经济利益, 有 66.47% 的受访者认为大数据“杀熟”侵犯了个人信息保护权。此外, 基于情感定向的精准推荐也在不断突破用户消费的心理防线, 个人信息披露往往能带来即时的好处(如: 注册会员即享优惠), 但当对方太了解我们时, 我们就失去了自主权。<sup>[34]</sup> 总而言之, 与网络服务提供者所掌握的信息和技术优势相比, 用户的劣势地位导致了其在风险感知和预判上的滞后。所以在与网络服务提供者的协商沟通中, 用户更容易被所谓的个性化内容观点所裹挟, 从而成为数字建构中被“捕获”的个体。

## 四、以信息赋权推进自主性构建: 算法推荐中隐私问题的规制路径

### (一) 信息自控与自决: 算法推荐时代信息隐私管理的理论原则

“自主性”来源于希腊词中表达自我管理、自我支配的概念, 其哲学范畴的内涵指代人根据自由意志进行自主活动的状态。<sup>[35]</sup> 数字时代算法推荐机制对人的自主性冲击主要表现为个人信息的“失权”危机, 而当前的信息“赋权”机制尚未有效确立与落实, 由此个人信息自由受到算法权力的操控。算法权力反作用于人类甚至统治支配人的现象被视为算法权力的异化,<sup>[36]</sup> 这构成算法推荐机制全面内嵌于人们社会生活的现实背景下, 应对技术风险需要解决的紧迫议题。概而言之, 算法推荐模式引发的

① 参见北京市消协发布大数据“杀熟”问题调查报告. [http://www.bj315.org/xyyw/xfwx/202209/t20220909\\_35059.shtml](http://www.bj315.org/xyyw/xfwx/202209/t20220909_35059.shtml)。



个人信息自主性冲击体现在对信息获取与信息分发的深度介入,作为信息输入端的算法能够实现个人信息的获取与分析处理,而作为输出端的算法则控制着信息需求匹配,由此建立用户与信息服务之间的精准连接。在此过程中,算法推荐机制替代了人的自主选择,商业利益驱动个人信息价值的释放,程序规则的全面嵌入更加助推了人的主体性危机。基于智能算法的精准推荐模式蕴含着与个人信息自由乃至信息自主相悖离的异化力量,这集中体现了数字时代算法推荐所带来的技术风险。

在以信息要素为基础的数字化社会,信息资源的获取与价值挖掘是网络服务提供者提升自身竞争力的关键,个人信息自主性问题由算法推荐机制所引发的信息与隐私权益受损而起。因而应对算法共生时代个人信息自主性危机,首先需要围绕信息与隐私的保护规范展开。个人信息作为算法系统运行的基础资源,决定了算法推荐机制的实际效力,而用户对个人信息的自控与自决则决定了其能在多大程度上实现信息自主。在基于“数据—算法”逻辑建构的信息流动机制中,自主性构建有赖于从两方面重塑用户的主体性:一是用户对其信息的自控,即个人依据其自身意志决定透露个人信息的行为,这是数字时代个人信息与隐私管理的核心内涵;二是个人自主决定信息触达,即意味着用户能够根据自身需求进行信息选择。这种“由内而外”的信息使用权和“由外而内”的信息选择权,共同构成了数字化社会中个人信息自主性的两大维度。因此,当前如何规范管理个人信息及隐私是关涉自主性构建的关键范畴,它既触及数字时代个人与其信息要素的所属关系问题,也关乎实际运作中信息价值收益的合理分配,集中体现了技术风险语境下如何处理人的主体性问题需要思考的时代命题。

## (二) 透明公开与信息赋权:数字化社会中自主性构建的现实路径

在与算法共生的时代,“信息赋权”旨在通过保障个人在其信息获取、处理以及使用过程中的主体性权益,形成用户主导的信息流动机制,以个人信息的自控与自决“倒逼”算法机制与信息处理的透明公开。早在 20 世纪 90 年代,欧盟就开启了个人信息的立法保护规定,<sup>①</sup>以应对互联网时代随之而来的个人信息权益问题。如今法律规制已成为数字化生存中应对个人信息与隐私问题的普遍选择,就现实路径而言,法律规制中合理界定个人信息范围是基础依据,相应的行业自律规约是有效落实的关键,形成多方协同的精细化规范体系是目标追求。

### 1. 推进差异化场景中的信息分类与风险分级

信息的实时流动使得动态场景下个人信息范围界定变得困难,信息识别性边界的模糊成为个人信息赋权亟待解决的问题。技术变革带来的个人信息与隐私保护挑战,主要在于动态的信息场景取代了以往静态模式下“二元化”的信息预判。信息赋权基础与构建自主性的现实路径,首先在于实现信息流动中的个人信息分类与隐私风险分级,推进动态场景导向的个人信息与隐私保护机制的构建。“场景导向”的理念源于尼森鲍姆的“情景脉络完整性”理论,<sup>[37]</sup>意在强调“尊重个人信息原始收集的具体场景,其后续传播利用不得超出原初的情景脉络”。<sup>[38]</sup>这种动态的个人信息保护理论框架在现有法律中已有所体现,例如 GDPR 在授权许可的基础上,增加了被遗忘权、数据携带权等,为个人提供了更加灵活的隐私信息管理方式;CCPA 引入了“选择退出”(opt-out)的方法作为授权原则的协同机制,只有在合理授权范围内的信息处理无需经由个人再次同意,而超出此范围则用户有权依据其合理隐私期待而选择退出,由此体现出差异化情景导向的隐私保护机制在信息流动场景中的适用性。

不同信息流动场景下的个人信息进行分类和风险分级,关涉到当前我们应该保护哪些个人信息这一核心问题,构成信息流动中个人信息与隐私保护机制趋于精细化的基础。例如我国《个人信息保护法》就针对敏感信息处理做出了专门规定,对于“一旦泄露或者非法使用,容易导致他人的人格尊严受

<sup>①</sup> 1995 年 7 月 24 日欧盟部长会议制定的《关于涉及个人信息处理的个人保护以及此类信息自由流动的第 95/46 号指令》(简称《个人信息保护指令》)

到侵害或者人身、财产安全受到危害”的敏感信息,不仅需要充分必要的获取目的,还需要有严格的保护措施,并且要获得个人单独同意,除此之外还需考虑未成年人敏感信息处理的特殊性;<sup>①</sup> GDPR 也对涉及九类个人敏感数据信息做出了“禁止处理”的特殊规定。<sup>②</sup> 伴随信息与通信技术的发展,个人数据信息类型变得更加丰富,敏感信息的范围也在不断拓展,更多的信息类型被纳入其中,由此被用以处理哪些信息需要进行保护的问题。<sup>[2]</sup> 这也表明,信息技术的进步也使得个人信息的内涵与外延发生变化,个人信息与隐私保护的理论框架也需要不断拓展和持续更新,未来需要基于动态场景理念,结合利益权衡原则,围绕信息内容、信息主体和信息价值等多维度,制定个人信息分类的细化标准,为信息流动中的隐私风险评估提供详细依据,从而推动制定个人信息与隐私保护的针对性方案。

## 2. 技术赋能行业自律与隐私管理

隐私管理是人们对其分享信息时机、对象以及内容等方面的考虑,<sup>[39]</sup> 当前由技术变革带来的个人隐私风险问题,也有赖于借助技术手段予以解决。既有的“授权同意”保护机制之所以沦为形式条款的核心问题在于:一是脱离差异化使用场景的“全有或者全无式”预判,以及同意或者退出的选择模式,用户难以在有效知情的情况下做出自主决策;二是面对过高的隐私管理成本和有限的用户理性,用户很难充分理解网络服务提供者发布的隐私条款,既无从判断其内容规则的合理性,也无法进行实现常态化的隐私风险评估与决策。因此,个人信息保护实践的推进有待于融入技术管理手段,完善差异化场景中分类信息的风险等级评估机制,以技术工具规避用户隐私管理的非理性误区,实现个人信息与隐私风险的实时监测与评估,并根据实际情况提供相应的解决方案建议。

首先,行业应加快构建个人信息保护的技术规范系统,依据动态场景差异为用户提供多元化的选择,从而为个人信息权益提供实质性的保护措施。例如美国互联网协会推出的“个人隐私选择平台”(personal privacy preference platform,简称“P3P”),为个人的隐私管理提供了灵活的选择空间,在一定程度上弥补了选择或退出的单向决策缺陷。其次,应运用技术手段为用户提供个性化的隐私风险评估与管理方案,鉴于网络服务提供者对个人信息的收集和使用涉及多个环节,个人信息与隐私保护应从信息流动的全流程予以考量,根据“信息生命周期”的不同和用户网络行为的差异,提供分阶段、分场景以及分类信息的隐私风险评估报告,既要说明其中的隐私风险,也要明确信息使用为用户带来的价值收益,从而根据利益权衡原则为用户提供相应的优化建议。另外,当用户遇到高隐私风险的网络服务应用时,应及时发布敏感信息泄露风险预警,从而提升用户的隐私风险意识。由此,通过技术赋能为个人信息与隐私管理提供科学合理的研判机制,用切实可行的简化操作方式,真正为个人信息与隐私保护带来实效。

## 3. 法律规制与自治协同构建精细化的规范体系

随着智能算法推荐成为社会运行的常态,构建相应的个人信息与隐私问题的规制体系已刻不容缓。由于算法推荐中的隐私问题关涉多主体、多环节和多方利益,且随着技术变革其动态化和复杂性与日俱增,个人信息与隐私保护机制的完善有赖于法律规制与自治的多方协同,推进理论框架与保护实践的有机融合。这不仅需要从欧盟的法律规制路径和美国行业自律模式中获得启发借鉴,而且要依据我国数字行业的发展阶段,逐渐完善我国个人信息与隐私保护的多方协同治理体系,规范网络服务中的个人信息收集和使用,从而打造良好的信息生态环境。

具体而言,首先需要从法律层面进一步完善行业个人信息保护特别法规体系,在以《个人信息保护法》为核心的综合性法律保护基础上,逐步构建更具针对性的行业特别法规体系。虽然综合性法律

① 参加《个人信息保护法》第二十八条: <http://www.customs.gov.cn/kjs/zcfg73/4265285/index.html>。

② 参见“General Data Protection Regulation”第9条,第1款: <https://gdpr-info.eu/art-9-gdpr/>。



具有系统而全面的优势,但也可能会面临细化层面的行业适应性问题,过于概括和抽象的内容难免存在实际应用的局限,这就需要针对行业特点制定相应的法律条款。我国《民法典》在个人信息保护与利用方面构成特别法;<sup>[40]</sup> 欧盟的《电子通信数据保护指令》、美国的《电子通信隐私权法》《家庭教育权利与隐私法》等<sup>[41]</sup> 都是针对特殊行业领域的专门法。我国各相关行业也需要依据法律规定,构建个人信息保护的行业自律规约机制和通用标准,这有赖于以中国互联网协会等为代表的行业力量,积极推动个人信息保护行业规范体系的建立,例如借鉴美国的行业自律机制,实施行业指引(suggestive industry guidelines)和在线隐私认证在线隐私认证(online privacy program),<sup>[20]</sup> 由行业联盟根据法律要求制定整个行业适用的隐私保护自律规范,并要求行业成员遵守和执行,同时也可以通过网络隐私认证机制,为符合隐私保护规范要求的网络服务提供者提供隐私认证标志,以使用户选择更能保障信息隐私安全的网络服务。再者,就个人信息保护的用户自治而言,在为用户提供相应的隐私风险监测、评估、解决及溯源问责路径的同时,也要注重个人信息素养的不断提升,增强个人信息与隐私保护的自我管理意识与自主性。总之,智能算法推荐时代的个人信息与隐私保护,有赖于从基础法律规制、行业自律和个人自治层面协同推进,构建有机融合的多元并行框架,从而为信息商业价值应用与个人信息及隐私权益保护的合理权衡提供可行路径,以期促进透明化生存时代个人信息自主性构建。

## 五、结 语

信息要素作为一种社会资源已经成为当前数字化社会运行的必要基础,信息流动不断革新传统的个人信息与隐私内涵,算法机制的深度内嵌使得透明化生存中如何构建个人信息自主性成为新的时代命题。伴随着信息技术发展潮流,数据和算法愈发成为行业创新发展的核心驱动力量,数字化社会的矛盾与冲突也日益围绕信息资源及其价值挖掘展开。个人信息与隐私的商业化利用中所显现的个人自主性危机,集中反映了算法技术的工具理性所带来的人文价值的冲击。由于个人信息与隐私保护关乎个体人格权益、经济效益以及社会的长足发展,其不仅涉及技术、经济、法律等多元社会议题,且相应保护机制的建立也面临多方社会主体利益的调和与博弈。如今我国的个人信息与隐私保护制度体系的构建进入关键时期,在结合国际经验,基于法制框架和行业自律路径,探讨信息商业价值挖掘与个人信息权益保护之间的有效平衡之外,未来更需要纳入多元主体视角展开研究,为技术变革背景下的个人自主性构建提供理论与实践指引。

## 参考文献:

- [1] Michelfelder, D. P. (2001). The moral value of informational privacy in cyberspace. *Ethics and information Technology*, 3 (2): 129-135.
- [2] 王敏. 大数据时代如何有效保护个人隐私——一种基于传播伦理的分级视角 [J]. 新闻与传播研究, 2018 (11): 69-92.
- [3] Goldfarb, A. & Tucker, C. (2011). Online display advertising: Targeting and obtrusiveness. *Marketing Science*, 30 (3): 389-404.
- [4] Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, 51 (5): 546-562.
- [5] 于婷婷, 杨蕴焄. 精准广告中的隐私关注及其影响因素研究 [J]. 新闻大学, 2019 (9): 101-116.
- [6] Goldfarb, A. & Tucker, C. (2011). Privacy regulation and online advertising. *Management Science*, 57 (1): 57-71.
- [7] Romanosky, S., Telang, R. & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft. *Journal of Policy Analysis and Management*, 30 (2): 256-286.
- [8] Goldfarb, A. & Tucker, C. (2012). Privacy and innovation. *Innovation Policy and the Economy*, 12 (1): 65-90.
- [9] Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, 4 (5): 193-220.

- [10] Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.
- [11] 王四新, 周净泓. 网络空间隐私权的保护研究——基于公共场所隐私权理论 [J]. 四川理工学院学报 (社会科学版), 2018 (6): 22-36.
- [12] [美] 汉娜·阿伦特. 人的境况 [M]. 王寅丽, 译. 上海: 上海人民出版社, 2017: 32.
- [13] 顾理平, 王颀濛. 从圈子到关系: 智媒时代公私边界渗透及隐私风险 [J]. 社会科学辑刊, 2022 (3): 184-190.
- [14] 向秦, 高富平. 论个人信息权益的财产属性 [J]. 南京社会科学, 2022 (2): 92-101.
- [15] 鞠宏磊. 大数据时代的精准广告 [M]. 北京: 人民日报出版社, 2015: 184.
- [16] 张红春, 章知连. 从算法黑箱到算法透明: 政府算法治理的轨逻辑与路径 [J]. 贵州大学学报 (社会科学版), 2022 (4): 65-74.
- [17] 吴椒军, 郭婉儿. 人工智能时代算法黑箱的法治化治理 [J]. 科技与法律 (中英文), 2021 (1): 19-28.
- [18] Hodges, L. (1994). The journalist and privacy. *Journal of Mass Media Ethics*, 9 (4): 197-212.
- [19] 王泽鉴. 人格权的具体化及其保护范围·隐私权篇 (上) [J]. 比较法研究, 2008 (6): 1-21.
- [20] 齐爱民. 个人信息保护法研究 [J]. 河北法学, 2008 (4): 15-33.
- [21] 任龙龙. 个人信息民法保护的理论基础 [J]. 河北法学, 2017 (4): 181-192.
- [22] 程德理, 赵丽丽. 个人信息保护中的“识别”要素研究 [J]. 河北法学, 2020, 38 (9): 44-54.
- [23] 陈堂发. 互联网与大数据环境下隐私保护困境与规则探讨 [J]. 暨南学报 (哲学社会科学版), 2015 (10): 126-130.
- [24] Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, 126 (7): 1880-1903.
- [25] 邵国松, 杨丽颖. 在线行为广告中的隐私保护问题 [J]. 新闻界, 2018 (11): 32-41.
- [26] 顾理平. 无感伤害: 大数据时代隐私侵权的新特点 [J]. 新闻大学, 2019 (2): 24-32.
- [27] 周佳念. 信息技术的发展与隐私权的保护 [J]. 法商研究, 2003 (1): 25-32.
- [28] 徐敬宏, 赵珈艺, 程雪梅等. 七家网站隐私声明的文本分析与比较研究 [J]. 国际新闻界, 2017 (7): 129-148.
- [29] 袁梦倩. “被遗忘权”之争: 大数据时代的数字化记忆与隐私边界 [J]. 学海, 2015 (4): 55-61.
- [30] Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review*, 53 (6): 1393-1462.
- [31] Richards, N. M. & King, J. H. (2013). Three paradoxes of big data. *Stanford Law Review Online*, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2325537&rec=1&srcabs=1926431&alg=1&pos=566](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325537&rec=1&srcabs=1926431&alg=1&pos=566): 41-46.
- [32] 严炜, 邹盼. 面向大数据技术的隐私困境思考 [J]. 江汉论坛, 2016 (8): 65-70.
- [33] 胡元聪, 冯一帆. 大数据杀熟中消费者公平交易权保护探究 [J]. 陕西师范大学学报 (哲学社会科学版), 2022 (1): 161-176.
- [34] Acquisti, A., Taylor, C. & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54 (2): 442-492.
- [35] 马衍明. 自主性: 一个概念的哲学考察 [J]. 长沙理工大学学报 (社会科学版), 2009 (2): 84-88.
- [36] 赵一丁, 陈亮. 算法权力异化及法律规制 [J]. 云南社会科学, 2021 (5): 123-132.
- [37] Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, 79 (1): 119-157.
- [38] 范为. 大数据时代个人信息保护的路径重构 [J]. 环球法律评论, 2016 (5): 92-115.
- [39] [美] 斯蒂芬·李特约翰. 人类传播理论 [M]. 史安斌, 译. 北京: 清华大学出版社, 2004: 293.
- [40] 任愿达. 《民法典》个人信息保护规定与数据资产治理理念的协调路径 [J]. 西南民族大学学报 (人文社会科学版), 2022 (6): 114-123.
- [41] 翟羽艳. 我国隐私权法律保护体系存在的问题及其完善 [J]. 学习与探索, 2019 (10): 80-84.

[责任编辑: 华晓红]