DOI:10.3876/j.issn.1671-4970.2023.06.002

数字身份的泛在形态及其伦理风险治理研究

张　峰,杨　丽

(华中科技大学马克思主义学院,湖北 武汉　430074)

摘要:数字身份是以数字化形式存在的身份形态,与网络空间相伴而生。网络无处不在、无时不在的泛在特征使数字身份呈现出云形态、微形态、超文本形态、可视化形态和碎片化形态,为人们生产生活带来便利的同时,也在一定程度上存在伦理风险。数字身份的不合理应用总体指向了认同、隐私、自由和正义等4个伦理议题:数字身份弱化了人的自我认同和社会认同,造成了"整合型隐私"保护困境及"隐私悖论",遮蔽了主体的自由意志和社会遗忘能力,隐含了"数据偏差"和"算法逻辑"不正义等问题。随着互联网日益普及,传统身份逐步向数字身份转型,加强数字身份伦理风险治理成为重要的时代议题。在新发展阶段,应充分利用技术、法律、伦理的协作互动,实现数字身份伦理风险的协同治理,提升数字社会认同感,维护数字身份隐私权,克服数字身份的异化,消解算法逻辑的歧视性影响,使其更好服务于社会政治经济发展和满足人民的美好生活需要。从技术治理层面来看,要加强技术的创新和发展,克服技术自身存在的负效应;从法律治理层面来看,应坚持权利与义务辩证统一的立法原则,为数字身份应用提供法律保障;从伦理治理层面来看,各个主体要加强自我约束,自觉成为数字身份治理的重要补充力量。

关键词:数字身份;泛在形态;伦理风险;协同治理

中图分类号:B082　　**文献标志码**:A　　**文章编号**:1671-4970(2023)06-0009-10

凡人皆有身份,从社会学意义上讲,身份是指人在社会体系中的位置识别;从法学意义上来讲,身份是指人的权利和义务的能力的总和[1]。数字身份是网络时代出现的有别于传统身份的新的身份类型,是"在网络环境下,由个体在线活动提供,能被检测到或被数据算法得出的所有能表明主体身份信息的数据聚合体和数字化映射。"[2]显然,数字身份的网络空间特性决定了其存在形态的泛在性。"泛在"(ubiquitous)概念的引入源于20世纪90年代,最先由美国施乐帕洛阿尔托研究中心首席科学家维瑟博士提出,被用来形容网络无处不在、无时不在的特性,后来衍生出"泛在网"概念,即无所不在、无时不在的网络。数字身份是网络发展的产物,其泛在形态具体表现为云形态、微形态、超文本形态、可视化形态和碎片化形态。数字身份的网络泛在性引起了人们生产生活的数字化变革,催生了电子政务、数字经济、网络文化、虚拟社交、数字生态等新兴领域,开拓了虚拟空间、虚拟实践和虚拟劳动的新场域。不过,数字身份在为人们生产生活带来便利的同时,也产生了一系列伦理问题。数字身份的认同问题、隐私问题、自由问题和正义问题等伦理议题是学界亟须重视的关键问题,对于建设和谐的数字社会、智慧社会具有底层逻辑的意义。

引用本文:张峰,杨丽.数字身份的泛在形态及其伦理风险治理研究[J].河海大学学报(哲学社会科学版),2023,25(6):9-18.

基金项目:中央高校基本科研业务费专项资金资助项目(2015AA020);华中科技大学自主创新研究基金(人文社科)重点专项项目(2015AE025)

作者简介:张峰(1958—),男,教授,博士,主要从事马克思主义理论和大数据哲学研究。E-mail:zhangfeng581215@163.com

一、数字身份的泛在形态及其伦理向度

据中国互联网络信息中心第 52 次《中国互联网络发展状况统计报告》显示,截至 2023 年 6 月,我国网民规模达 10.79 亿人,互联网普及率达 76.4%[3]。随着互联网普及程度越来越高,传统身份正在向数字化身份转型,呈现为云形态、微形态、超文本形态、可视化形态和碎片化形态,泛在化的数字身份也在一定程度上重塑了身份与主体、记忆与遗忘、现实与虚拟、内容与形式的关系。

1. 云形态

数字身份的云形态是指将数字身份信息存储在云计算平台,实现身份信息的在线化、集中化和共享化。区别于传统的“中心式”存储结构,当前海量的数据存储采用“分布式”结构,数据存储设备从“单个的固定的”硬件转变为由众多存储设备和服务器所构成的“云”[4]。一方面,数字身份的云形态可以实现安全而稳定的身份存储,减少本地设备损坏、数据丢失等不确定性因素带来的身份信息风险;另一方面,数字身份在云平台上的存储和管理,可以实现身份信息在不同时间维度的实时同步、更新和在异质空间维度的彼此交互共享,促进更加便捷和高效的数字社会互动。

数字身份的云形态重塑了时间的概念,解构了记忆与遗忘的关系。在数字时代,一键清空自己的聊天、购物和搜索记录是一件很容易的事,但要删除同步在“云”端的数据则几乎是不可能的。随着存储手段的精进和身份信息数字化的程度越来越深入,个人身份信息将会永远存在“云”上。具有永生性的“云”信息,让人们失去了删除的权利,也丧失了遗忘的能力。在存储技术匮乏的时代,记忆的成本总是高于遗忘的成本,人们穷尽各种本能和媒介来记忆却总是抵不过时间,“而数字时代颠覆了这一切”[5]23,数字身份信息的存储成本远低于清理成本。

2. 微形态

数字身份的微形态是指人们以“微”型身份在虚拟数字空间进行聊天、购物、娱乐、学习等活动,具有实时的快捷性和“个体在场”的临场感。数字身份带人们迈入了微时代,跨进了微空间,并形成了带有微型、快捷、海量和多场景价值特征的微文化。与传统的身份形态相比,这种虚拟的“微身份”更具灵活性和多样化,适应了人们在移动互联网、物联网等多种场景下的数字身份需求。另外,数字身份的微形态突出表现在“微群”,基于现实联系人的强关系组成新的“朋友圈”,借助群体传播的优势从它们“自然存在的‘动态能力’中汲取能量和刺激”[6],大大延长了人们的社交半径。

数字身份的微形态拓展了人们的生存空间,重塑了身份与主体的关系。在数字时代,人们的生存空间从实体世界扩展到虚拟世界,但主体的经验却无法简单地复制和平移,只有当借助技术手段实现自身的数字化转型后,人们才能开展正常的虚拟社交和虚拟实践活动。因此,生活在数字时代的人们不仅拥有实体身体,还拥有一个活跃在虚拟空间的虚拟主体。随着数字身份越来越具有自主性,人的主体性将面临全方位的撕裂乃至坍塌的危险。

3. 超文本形态

数字身份的超文本形态是指将数字身份信息通过超文本技术呈现出来,以便用户更加灵活地访问、组合和分享自己的数字身份信息。纳尔逊创造了“超文本”这一术语,将其定义为一种非连续性写作[7]。一方面,超文本通过链接等技术将不同文本、图像、音频、视频等信息进行互联和组合,实现了线性与非线性、逻辑与非逻辑、结构化与非结构化信息的跨界面交互融合[8];另一方面,超文本的多样化和灵活性特征拓展了人们自由活动的空间,也增强了数字身份的信息自由度,在一切可及都可以数据化的技术语境下,“所有的存在物都将被纳入文本”[9]。

数字身份的超文本形态扩展了身份信息的维度,其内容与形式的关系将迎来重大变革。超本文凭借超强的交互融合技术,主宰了当前的信息文化传播环境。图片、音频和视频等超文本正日益取代传统的文本文字,成为人们主要的信息接收方式和传播方式。超文本语境下令人眼花缭乱的呈现形式逐渐将读者的重点吸引到肤浅的形式阅读,也将人们的消费需求转

向更加注重潮流趋势和多变风格的标新立异，猎奇的新鲜感和体验感已经超越了内容本身的价值，并隐含了“超文本变异”的伦理风险。

4. 可视化形态

数字身份的可视化形态是指利用数字技术将身份信息整合并以文字、数据、图表、画像、声音和视频等多种方式融合呈现的可视化效果。可视化的历史可以追溯至史前时期，人类结绳记事对社会生活进行了有效记录，而现在的可视化主要是指将数据以图形或图像等视觉方式呈现出来的现代技术、方法和理论。一方面，可视化是数据得以被人们理解的语言和工具，人类对外部信息的接收有 80% 以上源于视觉[10]，对海量、非结构化和多维度的数据进行可视化呈现，不仅能够洞悉数据背后的规律获得更多的“附加值”[11]，还能通过视觉效应打造“用户沉浸式体验”的多场景价值[12]；另一方面，可视化技术通过勾画个人“身份画像”，以动态化的、立体的数字语言丰富了平面化的二维空间的文字语言，利用数字符号和数字媒介实现了生动而形象的身份呈现。

数字身份的可视化不仅是对身份的类型化构建，也削弱了个体在身份构建上的自主性。一方面，数字身份可视化的实质是将身份信息转化成数据并根据社会既有标签进行分类赋值，表明其潜在的价值和可能存在的风险。可视化的“身份画像”是依据数学模型来进行数据分析的，不可避免带有片面性，甚至可能基于不平等的标准进行分组，实行分类管理和区别对待。另一方面，整个数据化和社会分类过程是在“黑箱”中进行，每个被分析的主体完全意识不到从自己身上收集到的数据，是如何分类、“画像”以及最后被用作何种用途的。这种不透明的数字身份构建过程，让用户失去了定义自己身份的自主权。

5. 碎片化形态

数字身份的碎片化形态是指数字身份信息在网络环境下呈现出来的一种分散的、不连贯的形态。碎片化的原意是完整的东西变得零碎，在现代化和后现代化语境中，出现了“信息碎片化”“语境碎片化”和“受众碎片化”的现象[13]。从人类社会发展角度来看，随着社会分工日益精细，社会结构在专业不断细分的背景下不可避免地会呈现出碎片化特征。到了数字化时代，数字平台与社会生产生活的融合日益深入，数字社会的分工更是渗透到了个体层面，数字身份在参与数字平台的生产生活实践中也逐渐被碎片化。微信存储社交信息、淘宝存储购物信息、美团存储娱乐和美食信息，人们甚至还可以基于不同需求形成不同的数字身份，并随时间、空间和环境的变化随时变更。这种去中心化的数字身份形态在一定程度上释放了更多的活动空间，但由此造成的信息闭塞现象也容易导致社会各主体对数据资源占有和使用程度的不对称。

数字身份的碎片化形态不仅解构了时间和空间，也让人们形成了碎片化的生存方式。一方面，数字身份的碎片化破坏了人们知识体系的完整性、日常时间的连贯性、工作内容的延续性以及交往的社会互动性，这对人的注意力造成了损耗，进而瓦解了人们深度思考的能力；另一方面，人们对数据资源占有和使用程度的不同造成了“数字鸿沟”现象，此种现象本质上是一种“技术鸿沟”，但其最终指向的是社会的公平正义。数字技术的高速发展并没有弥合“鸿沟”，反而造成了“富者越富，穷者越穷”的恶性循环，最终必然危及社会的公正与民主[14]。

二、数字身份伦理风险的重点议题

数字身份的泛在形态实现了主体、时空和实践等多维度的变革，为人们生产生活带来了丰富的体验和无数的便利，同时也在一定程度上破坏了传统伦理的生存土壤，无论是从个体视角还是群体视角都存在潜在伦理风险。综合数字身份云形态、微形态、超文本形态、可视化形态和碎片化形态潜藏的伦理风险因素，数字身份的伦理风险总体上指向 4 个重点议题，即认同、隐私、自由和正义。

1. 认同危机：数字身份弱化了人的自我认同与社会认同

认同与身份是相伴而生的，认同的英文是“identity”，中文翻译就同时包含了“认同”和“身份”的含义[15]。认同产生于主客体关系中人的自我同一性，因此认同的基础是“自我认

同”。之后,泰弗尔等提出了“社会认同”的概念,认为社会认同本身是一种集体观念,是社会成员共同拥有的信仰、价值和行动取向的集中体现,而且注重归属感的社会认同更加具有稳定性[16]。无论是自我认同还是社会认同,总是在一定的社会互动中形成的,“人的本质并不是单个人所固有的抽象物,在其现实性上,它是一切社会关系的总和。”[17]139 随着数字技术的产生和发展,传播变量中“空间、时间和物理障碍”的因素变得越来越不重要[18],片段化的数字身份瓦解了主体的完整性和身份发展的一致性,进而导致人的独特性丧失和人的个体性被过分放大,长此以往,人们将陷入身份认同的危机。

数字身份的生成依托特定的算法技术,这就决定了数字身份的叙事必然受制于某种算法逻辑,而程式化的算法逻辑注定是与人所追求的独特性价值背道而驰的。依托数学集合中的可度量数据元素建立的数字身份本质上是一种类属身份,忽视了“以人类为中心的叙事、语境和历史”[19]51,人的情感、经验、阅历和主体性差异等本真属性都被扁平化了。借助美国学者利波尔德的“可度量类型”概念,可度量类型是一种被用来赋予用户某个身份的数据模板,而能否被赋予类属身份取决于是否与算法匹配[19]48。在这种“类型化身份”的生成过程中,人区别于他人的独特性价值被逐渐解构。数字身份时代更强调规律性而不是变化性,更突出一致性而不是差异性,更彰显匹配度而不是个性化,人们很容易陷入“标签化”和“同质化”的身份设定,这让数字身份时代的人没有了独特性,数字社会也逐渐缺乏多样性。这种类型化的身份特征“将人还原为物的存在,以物确定人的社会身份”[20]110,人与物的关系又仿佛回到了古希腊哲学中人与物同源同性的状态,“人之为人”的伦理本质在大数据的表证中被消解。

与人的独特性丧失相反,数字身份时代人的个体性又容易被无限放大。过分强调人的个体性无疑会助长个人主义的不正之风,“社会认同问题的提出实际上是对现代西方社会个人主义价值观的纠偏”[21]。数字身份在虚拟空间的建构缺乏应有的监管和约束,这致使人们更偏向强化数字身份的认同而忽视了与现实身份的一致性,从而造成数字身份与现实身份的疏离甚至人格分裂,导致数字身份与现实身份主体在道德品格和行为准则方面产生矛盾。过度强化数字身份认同可能会滑向个人主义,威胁数字身份时代的社会认同。因此,平衡好数字身份和现实身份、自我认同和社会认同的关键是要回到实践,在实践中把握二者的辩证统一。马克思认为,“社会生活在本质上是实践的[17]135,人们要在实践中,也即是在劳动中获得自我身份的确证。”数字身份时代缺乏恰当的社会情景作为互动的背景,基于网缘关系建立的“集体”必然不会持久和稳固,人们也很难对其产生归属感。当现代文明将个体最高价值赋予自我之中时,不仅“加剧了个体的自我毁灭”,个人主义的无限泛滥也会使“社会处于无以复加的分裂之中”[20]67。

2. 隐私危机:数字身份的“整合型隐私”及“隐私悖论”

隐私对于个人的生存和发展具有重要价值,尊重和保护隐私是人类文明进步的标志。数字身份的实质是现实的人在进入数字空间过程中的身份让渡。在数字身份时代,人们的肉身并不直接参与交往,而是借助一个或多个数字化的身份参与交往。数字身份本身并不能承担主体责任也不能享有主体权利,其存在仅仅是“为数字世界确立行为主体”,本质是作为一个“可追溯性的身份”而存在的[22]。隐私权作为一项基本的人权,在传统身份向数字化身份的转型过程中也面临着权利让渡的风险,在主体知情或不知情的状况下,主体或主动或被动地放弃自己的部分隐私。数字技术的发展和数字身份的产生在给人们带来经济效益的同时,也使个人隐私保护面临前所未有的挑战。

数字身份时代的隐私是一种“整合型隐私”,从不受打扰或免于侵害的权利变成了一个动态发展的概念,即“通过数据挖掘技术,将人们在网络上留存的数字化痕迹进行有规律整合而生成的隐私”[23]。在数字身份信息的分析整合过程中,整体与部分的关系具有了新的内涵,大数据对隐私的影响“不仅仅是 1+1=2,很多时候是大于 2 的”[24],一些看似杂乱无序的

个人信息被整合并推算出个人隐私的事例不胜枚举。这种动态的“整合型隐私”主要有两个生成路径:一方面,为了享受一定的数字红利、实现数字交往的互动和虚拟自我的认同,人们可能主动放弃部分个人隐私;另一方面,平台通过各种隐蔽的算法技术来收集人们在网络活动中留下的数字足迹,并为其勾勒详细的“身份画像”,从而实现个性化推荐的目的,深度的数据挖掘和数据分析过程极易造成隐私泄露,虽然这并不一定是主观造成的结果。这种被动收集个人信息的方式是数字身份隐私被侵犯的主要途径,主要包括搜索引擎、数据库、摄像头、指纹识别、人脸识别等方式。人们在不知情的情况下被收集了身份信息并进一步提取到个人隐私,所有这些被动收集或主动暴露的隐私信息一起造就了隐私泛滥的现状。

在数字身份时代,媒介技术和隐私的关系存在着人们对隐私的私密性要求和媒介发展带来的信息公开的矛盾,而且随着数字身份的普及程度和媒介技术的发展程度愈高,这种矛盾将愈突出。同时,在媒介技术与隐私的矛盾交织中,人自身也陷入了矛盾:一边追求私人空间,一边又主动放弃部分隐私来换取便利,这形成了数字身份时代的“隐私悖论”。数字身份时代,人们已然无法保护隐私周全,那这是否就意味着应该降低对隐私保护的标准或者干脆放弃自己的隐私呢?“后隐私运动”认为隐私会阻碍信息的分享,人们应该主动放弃隐私,但义务论和后果论等主流伦理学观点仍然坚持要保护隐私[14]。关注隐私是人的天性,但这并不意味着毫无退让的可能,如果处在能让自身获益的特定情境下,个体也是有可能主动让渡部分隐私的,只是这个让渡应经由身份主体自主授意并在公开透明的过程中具体展开,而非被强迫或在主体不知情的情况下被利用。因此,数字身份时代隐私保护的关键是要把握好个人隐私保护与适度让渡权利的尺度,各主体要在追求经济利益和预防伦理风险中找到平衡点,而非“一刀切”地保护隐私或者完全放弃隐私。

3. 自由危机:数字身份遮蔽了主体的自由意志和社会遗忘

自由是人们永恒的追求,关于自由的定义多达数百种,但其核心主旨是一致的,都内含着“不受限制而能够按照自己意志行动”的意蕴。在马克思那里,人的自由问题就是人的发展问题,人的自由的发展同人类社会本身的发展是一致的,“每个人的自由发展是一切人的自由发展的条件”[25]。因此,探讨自由问题必须从个人和社会两个层面展开。在一定程度上,“每个正常的成年人都是自由的个体,拥有决定自己行为的自由意识”[26]176,但在数字身份时代,每个人都深陷“时间和空间的圆形监狱”[5]159,人们生产了数据却反被数据所支配、奴役,数字身份的异化致使人们丧失了对身份信息的掌控能力,遮蔽了主体的自由意志和社会遗忘能力,最终引发自由危机。

数字身份的自由危机可以回溯到福柯的“全景敞视主义”和波斯特的“超级全景监狱”。全景敞视建筑是一种“残酷而精巧的铁笼”,通过在被囚禁者身上“造成一种有意识的和持续的可见状态”来确保“权力自动地发挥作用”[27]226。相较于“全景敞视主义”,“超级全景监狱”的监控和规训手段则更加具有隐蔽性。在“超级全景监狱”中,数字身份是电脑之间交流的基础,借由数字身份,人们所有的日常活动都纳入被监视的范围,身份在不知不觉中演变成了一种“囚犯居民的身份”。数据库给每一个人都构建了数字身份,而且“全然不顾该个体是否意识到这种构建”[28]。现代社会的监控手段已经发生了无数变种,“个别观察、分门别类,以及空间分解组合”等规训原理以更隐蔽的形式呈现出来,通过一系列不露痕迹的操作造成惩罚体系的替嬗,让我们身在其中,心安理得[27]228。在数字身份逐渐普及的今天,人们接收的所有信息都蕴含着算法逻辑,短视频平台生成的个性化娱乐推荐、美食平台生成的个性化美食推荐、新闻平台生成的个性化时事新闻推荐都是算法运作的结果。总之,在不知情的情况下,算法勾勒了人们的“身份画像”,决定了人们所处世界的轮廓以及思维所能可及的边界。

最重要的是,这种严密的监控体系会让人们潜移默化地形成自我约束的机制,无形地被一种隐形的权力所控制,不仅失去了时空上的

自由,甚至丧失了遗忘的能力。一方面,随着人的身份从现实空间向数字空间的“脱域”,工作的条件从“在场”转向了“在线”。即使在闲暇时间,人们的注意力也逐渐被网络平台掠夺,数字身份挤占现实身份时间和空间的现象愈发严重,人们自由意识的阵地逐渐失守。另一方面,数字身份信息可以永续存在于“云端”意味着人们将不再会有遗忘,没有遗忘的人们就将永远被囚禁在数字化记忆的“超级圆形监狱”之中,这对于个人的自由全面发展是极其有害的。“遗忘不仅仅是一种个人行为,我们这个社会也会遗忘。”[5]21社会遗忘机制能够给那些曾经失败过和犯过错误的人第二次机会,能够重新接纳随着时间不断发展的人们。人是动态发展的,辩证地看待人的发展过程也是遵从人性的体现。在完整的数字记忆时代,人们要记得如何去遗忘,既要从过去吸取经验教训,又要坚定走向未来,唯有如此才能取得持续的发展和进步。

4. 正义危机:“数据偏差”和“算法逻辑”中的不正义之维

在原始社会对劳动成果进行分配伊始,人们就开始了关于正义的讨论。罗尔斯提出了一般的正义观:“所有社会价值——自由和机会、收入和财富、自尊的基础——都要平等的分配,除非对其中一种价值或所有价值的一种不平等分配合乎每一个人的利益。”[29]整体来看,正义要求社会按照一定的规范和标准来分配社会利益和承担社会义务,这种标准应当以平等为原则,标准的制定者和施行者应保持客观中立的态度。党的十九届四中全会明确将“数据”增列为继“劳动、资本、土地、知识、技术、管理”之后的第七大生产要素[30],并且是最先进、最活跃的生产要素。进入数字身份时代,对数据资源的平等分配和对数据信息的普遍可及成为人们的基本价值诉求之一。要实现数字身份时代的公平正义,就必须做到“任何人都不应当被排除获得参与社会生活所必需的资源,被排除从这些资源中获得好处”[31]。

数字身份时代,个体所获得的数据资源以及从数据资源中的获益并不是平等的。大数据分析范式的“数据偏差”会造成隐形的社会不公,基于整体而非个体的分配会让“少数人”遭受不公正的待遇。在数字化时代,数据的收集和处理变得更加简单,舍恩伯格更是直接指出大数据是“采用所有数据的方法”[32],他认为当样本量足够大的时候,可以实现“样本=总体”。但将整体性直接推广到个体身上,会导致个体的正义维度被淹没。现实中,个体命运总是被基于整体的大数据决策所牵动,个体难以避免地会因为大数据“偏差”而遭受不公,只是这种不公因为有大数据的背书而显得更加隐蔽。此外,“数据捕获”过程中的“平台单一性”也会造成同样的后果。某个或某类应用程序和网站中所呈现出来的人员数据,仅仅只能指向某个时刻正在使用该应用程序和网站的那些人,但如果取样的样本量足够大,人们会倾向于认为,可以推广到社会更加广泛的人群甚至是覆盖所有人群,这种以整体代表个体的做法也会产生带有不正义的结果。因此,数字的大小和数量的多少并不代表着可推广性,人们的视野绝不应局限在数理逻辑下。正如“电车难题”所反映出来的问题:人的权益决不能简单粗暴地以数量多寡、价值大小的数理化逻辑来评判。

数据本身是中立,但作为数据分析手段的“算法”却不是中立的。数字身份时代,算法逐渐走向与资本的合谋,引发了新一轮的“社会分类”和“社会分化”。数据掌控者的权力迅速扩张,甚至侵犯了传统国家公权力和个人私权力的领地,解构了传统社会的价值秩序。传统社会以卓越的个人能力和突出的社会成就为荣,具有一定名气的人物往往都是各领域的佼佼者,他们历经时间的沉淀,跨越空间而传播,成为大众称赞和追捧的对象,而且成就越大、影响愈是深远。但现在的“名人”往往与“流量”挂钩,这些“流量”即算法逻辑入侵的结果,其所呈现的巨大热度和关注度背后实质是资本的较量。明星形象是靠媒体文本打造和包装出来的,“造星场域也是权力运作的场域”,明星效应对社会大众的影响和形塑是巨大而深刻的,控制了名人形象,也就相当于控制了社会性的人理解自己和世界的方式,因此这些潜在的影响也构成了身份的“原材料”,如今流量至上的风气甚至形成了以“流量”为标准的新一轮的社会分化和阶级固化[19]3。

三、数字身份伦理风险的协同治理

针对数字身份不合理应用所引发的认同危机、隐私危机、自由危机和正义危机等一系列伦理风险的治理，是坚持以人民为中心发展思想的必然要求。数字身份伦理风险的治理路径，不能依靠现有制度“自上而下”地演绎，而要“自下而上”地从问题出发来解决[26]247。一般来讲，技术的负效应主要是技术本身的缺陷或人们不恰当地使用造成的，相应的治理思路也应该从对技术的完善和对使用过程的约束入手。具体而言，可以借助技术本身的发展、法律制度的规约以及道德伦理的约束等三重合力实现数字身份伦理风险的协同治理，使其更好地服务于社会政治经济的发展和人民美好生活的实现。

1. 基于技术、法律和伦理的协同治理思路

第一，技术治理，通过技术进步克服数字身份应用的负效应。当前的数字技术正影响着人们生产生活，从个人到社会都被圈进数字场景革命，但任何技术都有其固有的不确定性，技术开发者也无法完全预知技术使用过程中的所有问题，因而数字身份的应用必然是一把“双刃剑”。在数字身份逐渐普及的时代，人们必须对其底层技术有着深刻的认识才能尽量规避其应用中的负效应。乌尔里希·贝克的风险社会理论对数字身份伦理风险的治理具有重要启示意义，其将科学划分为“初级科学化”和“反思性科学化”两个阶段，并指出第二阶段的科学需要直面自己的“产物、过失和二次问题”，这个阶段的进步在于将科学的质疑精神扩展到“科学自身的固有基础和外在结果”[33]190。而且，贝克认为科学的副作用是可以进行评估的，需要一种可以把“科技活动不可预测的副作用”置于关注的中心的理论[33]222。简言之，科学技术自身的缺陷可能是引发风险的因素之一，但技术的进步也是解决风险的重要手段。数字身份伦理风险的有效防范离不开网络技术和大数据技术的创新和发展，不能因为技术使用过程中产生的负效应而盲目拒绝技术本身，在发展中求得平衡才是应有的化解之道。

第二，法律治理，坚持数字身份权利与义务辩证统一的原则。法律是调整社会资源配置、平衡利益冲突、保障权利实现的重要手段，运用法律来规范技术是底线思维的运用。从法律视角去审视数字身份创建、存储、管理和运用的各个环节，会涉及诸多侵权行为，主要是侵犯了数字身份主体的知情权、隐私权、所有权和遗忘权等。目前，我国已经形成了以《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《个人信息保护法》三法为核心的网络法律体系，为数字身份时代形成良好网络生态提供了基础制度保障，但目前三法体系中精确涉及数字身份权利的内容较少，类似“被遗忘权”这种在国际国内司法领域都备受争议的新型数字人权更是无从涉及，且已有的三法体系多以数据权利的保障为主，缺乏对相关数字身份主体义务的规定。在数字身份伦理风险的法律治理层面，需要认识到数字身份的伦理风险既与数字身份权利的缺位有关，又与对数字身份义务规定的模糊不清有关。尼葛洛庞帝曾强调，“大多数的法律都是为了原子的世界而不是比特的世界制定的”[34]。作为“比特世界”的产物，数字身份在运用的过程中必然会出现非常多新的法律漏洞，因此必须从法律层面对数字身份进行强制性规定，必须坚持数字身份应用过程中权利与义务辩证统一的原则。

第三，伦理治理，将各个主体的自我约束作为重要补充力量。“社会公众的伦理意识跟不上技术发展的脚步”是转型期社会易陷入危机的重要原因[35]。数字身份的伦理风险往往无法预测且瞬息万变，相较于制度和法律的硬性规定和时效上的滞后性，道德约束则更具灵活性，是一种柔性的软规则，更适用于化解数字身份不合理应用产生的伦理风险。道德约束主要依靠主体的道德自律，道德自律则主要源于个体内在的道德情感和道德理性。先天的道德情感和后天的道德理性是实现道德约束的底层逻辑，而道德约束从“何以可能”到“何以实现”的转化也离不开道德教育的作用。道德教育是唤醒人的道德情感与道德理性的重要路径，也是加速道德动机和道德目的形成的催化剂。“共善”是人类生活在一起的必然要求[20]50，依靠道德层面的自我约束来化解数字身份的伦理风

险,需要各个主体明确自己的“初始义务”[14],并在接受道德教育的过程中不断强化自身的道德情感和道德理性。总之,各个主体越是具有社会责任感、越是有高度的道德自律,就越能创建更可信的数字身份,构建更和谐的数字社会。

2. 化解数字身份伦理风险的具体治理路径

第一,打造可信数字身份,提升数字社会的认同感。数字身份的认同危机主要表现为自我认同感和社会认同感不足,这主要是由于片段化的数字身份破坏了身份的完整性和身份发展的一致性。针对数字身份认同危机的协同治理思路:首先,数字身份主体在登记注册的时候要上传最新的和最真实的信息,并根据实际情况及时补充和动态调整,增强信息的真实性和准确度;其次,国家法律部门要不断完善数字身份的相关立法和使用规范,同时加强对数字身份应用的实时监管,加大对数字身份造假和盗窃等不法事件的打击力度,维护数字身份的良好信誉度;最后,对于技术工作者而言,要不断完善数据加密技术、入侵检测技术、防火墙技术、信息认证技术以及病毒防护等底层技术的升级,并努力打通不同平台数字身份壁垒,提升数字身份的连贯性和一致性。足够的信息安全感是数字身份主体获得自我认同感和社会认同感的前提,只有打造更加可信的数字身份,人们才能更放心地使用数字身份,也才能真正化解数字身份的认同危机。

第二,警惕个人数据泄露,切实维护数字身份隐私权。数字身份的隐私危机主要表现为人们在融入数字社会的过程中或主动或被动地让渡自己的部分隐私,并且随着社会的数字化程度越来越高,人们让渡的隐私也将越来越多。针对数字身份隐私危机,协同治理思路如下:首先,树立新型隐私观,在依托数字身份进行工作、学习和娱乐等活动的过程中要警惕主动暴露个人隐私的行为,同时各企业和平台应当自觉遵守行业规则,在收集数字身份信息的时候要尽量征得主体的同意,尤其是涉及隐私的部分;其次,国家法律部门要继续完善对数字身份隐私权的相关规定,同时与各大企业、高校及媒体形成多级联动,充分依托全国科普日、科技活动周、全国科技工作日等活动载体,借助微信推文、短视频、微电影等媒介载体,面向全社会开展数字身份隐私权的法律知识宣传普及;最后,区块链技术的去中心化、分布式存储以及共识机制特性与理念,对于减缓人们对隐私的担忧具有革命性意义,利用身份信息的“不对称性”可以有效实现数字身份隐私权保护的目的[36]。

第三,克服数字身份异化,实现每个人自由全面发展。数字身份的自由危机包括个人和社会两个层面:从个人层面看,数字身份异化会遮蔽主体的自由意志;从社会层面看,数字身份时代的社会遗忘机制正面临前所未有的挑战,无论是个体还是社会都不可避免地陷入数字记忆的囹圄。针对数字身份自由危机的协同治理思路:首先,在享受数字身份红利的同时,也要高度警惕受到数据流量的裹挟,避免因接受过度同质化信息而陷入信息茧房的陷阱,进而丧失独立思考和自主行动的能力;其次,要在技术层面实现对重要身份信息的数据脱敏处理,阻断利用敏感数据进行信息溯洄的各种不正当行为,确保个人自由意志的实现和社会遗忘功能的有效发挥;最后,国家要加大监管力度,从法律和制度的层面明令禁止任何以打击报复或以牟利为目的身份信息获取行为,不断完善科技伦理违法违规行为的查处机制,及时肃清数字身份应用过程中的违法违规行为,营造科技向善的良好环境,实现数字社会的繁荣稳定和每个人的自由全面发展。

第四,消解算法逻辑歧视,维护数字社会的公平正义。数字身份的正义危机不仅体现在数据偏差带来的隐形社会不公,还表现为算法与资本合谋所引发的新的社会正义问题。针对数字身份正义危机的协同治理思路:首先,个体要不断提高数据素养,积极维护自身的切身利益,成为数字身份伦理风险治理的主动参与者,尽量避免个体正义被淹没在大数据群体决策,缓解数据偏差和算法逻辑所带来的社会不公问题。其次,政府应当平衡好经济发展与伦理风险的关系,警惕数理化逻辑的歧视性影响,在顶层设计预先嵌入知情同意、保护隐私、公平分配、共享共济、公开透明、平等参与等伦理原则[14],同时密切关注数字身份鸿沟中弱势群体的感受,设置和完善相应的补偿机制。最后,企

业主体要担负起大企业的责任和担当,一方面不断精进技术,降低技术的获得成本,实现数字身份技术的普遍可及;另一方面不断完善算法程序,兼顾数据收集和分析过程中的效率与公平,尽可能从源头上减少数据偏差和算法逻辑带来的伦理风险,确保每一个人的公平正义。

四、结　语

数字身份是未来身份的主流形式,更是元宇宙世界的唯一通行证。届时,数字身份将对主体、时间、空间和实践等维度进行更深层次的变革,同时也可能引发除认同危机、隐私危机、自由危机和正义危机之外的全方位的数字身份伦理风险。技术本身是中性的,但任何技术的使用都内含着一定的好坏、善恶以及对错的价值取向与价值判断,要用辩证的眼光去认识数字技术的发展,既要肯定数字身份对社会发展的正向推动作用,又要警惕其可能引发的伦理风险,在二者的辩证统一中实现造福全人类的价值目标。

参考文献:

[1] 陈国强主编. 简明文化人类学词典[M]. 杭州:浙江人民出版社出版,1990:260.

[2] 葛秋萍,王珏. 大数据技术应用中个人数字身份的伦理规制[J]. 中州学刊,2020(10):95-101.

[3] 中国互联网络信息中心. 第 52 次中国互联网络发展状况统计报告[EO/OL]. [2023-08-28](2023-12-09). https://cnnic.cn/n4/2023/0828/c88-10829.html.

[4] 安宝洋,翁建定. 大数据时代网络信息的伦理缺失及应对策略[J]. 自然辩证法研究,2015,31(12):42-46.

[5] 维克托·迈尔-舍恩伯格. 删除:大数据取舍之道[M]. 袁杰,译. 杭州:浙江人民出版社,2013.

[6] 雷金纳德·范李,马克·盖伦切尔,费尔南多·纳波利塔诺,等. 群[M]. 时娜,译. 海口:南海出版社,2010:37.

[7] NELSON T H. Complex information processing: a file structure for the complex, the changing and the indeterminate[C]//Proceedings of the 20th Annual ACM National Conference. New York: ACM, 1965: 84-100.

[8] 张峰,彭志飞. 大数据时代"人的信息身体"的维度探析[J]. 自然辩证法研究,2018,34(12):82-86.

[9] 孙玮,李梦颖. 数字出版:超文本与交互性的知识生产新形态[J]. 现代出版,2021(3):11-16.

[10] 任磊,杜一,马帅,等. 大数据可视分析综述[J]. 软件学报,2014,25(9):1910.

[11] COHEN J, DOLAN B, DUNLAP M, et al . MAD skills: New Analysis Practices for Big Data[J]. Proceedings of the VLDB Endowment, 2009,2(2): 1481-1492.

[12] 吴声. 场景革命:重构人与商业的连接[M]. 北京:机械工业出版社. 2015:28.

[13] 信险峰. 对"碎片化"一词的误用与误读——新媒体内容的另类完整分析[J]. 青年记者,2022(3):49-50.

[14] 邱仁宗,黄雯,翟晓梅. 大数据技术的伦理问题[J]. 科学与社会,2014,4(1):36-48.

[15] GLEASON P. Identifying identity: a semantic history[J]. The Journal of American History, 1983, 69(4):910-931.

[16] TAJFEL H,TURNER J C. The social identity theory of inter-group behaviour [M]//WORCHELS. Psychology of intergroup relations, Chicago: Nelson Hall,1986:7-24.

[17] 马克思,恩格斯. 马克思恩格斯选集:第 1 卷[M]. 中共中央马克思恩格斯列宁斯大林著作编译局,译. 北京:人民出版社,2012.

[18] 约书亚·梅罗维茨. 消失的地域:电子媒介对社会行为的影响[M]. 肖志军,译. 北京:清华大学出版社,2002:10.

[19] 约翰·切尼-利波尔德. 数据失控:算法时代的个体危机[M]. 张昌宏,译. 北京:电子工业出版社,2019.

[20] 窦立春. 身份的伦理认同[M]. 北京:北京人民出版社. 2019.

[21] 李萍. 论道德认同的实质及其意义[J]. 湖南师范大学社会科学学报,2019,48(1):57-63.

[22] 徐强. 拟像抑或真实:数字主体的身份确认[J]. 南京师范大学报:社会科学版,2022(1):152-160.

[23] 杨建国. 大数据时代隐私保护伦理困境的形成机理及其治理[J]. 江苏社会科学,2021(1):142-150.

[24] 涂子沛. 大数据[M]. 桂林:广西师范大学出版社,2012:162.

[25] 马克思,恩格斯. 马克思恩格斯选集:第 4 卷

[M]. 中共中央马克思恩格斯列宁斯大林著作编译局,译. 北京:人民出版社,2012:647.
[26] 杜严勇. 人工智能伦理引论[M]. 上海:上海交通大学出版社. 2020.
[27] 米歇尔·福柯. 规训与惩罚[M]. 刘北成,杨远婴,译. 北京:生活·读书·新知三联书店,2012.
[28] 马克·波斯特. 第二媒介时代[M]. 范静哗,译. 南京:南京大学出版社. 2000:69.
[29] 约翰·罗尔斯. 正义论[M]. 何怀宏,等译. 北京:中国社会科学出版社,1988:58.
[30] 中国共产党第十九届中央委员会第四次全体会议文件汇编[M]. 北京:人民出版社. 2019:47.
[31] 西斯·J·哈姆林克. 赛博空间伦理学[M]. 李世新,译. 北京:首都师范大学出版社,2010:69.
[32] 维克托·迈尔-舍恩伯格,库克耶. 大数据时代[M]. 盛杨燕,周涛,译. 杭州:浙江人民出版社,2013:39.
[33] 乌尔里希·贝克. 风险社会[M]. 何博闻,译. 南京:译林出版社,2004.
[34] 尼古拉·尼葛洛庞帝. 数字化生存[M]. 胡泳,范海燕,译. 北京:电子工业出版社,2017:237.
[35] 吴瑾菁,陈颉. 大数据时代信息伦理的挑战与反思——以马克思主义权利观为视角[J]. 河海大学学报(哲学社会科学版),2022,24(2):22-29.
[36] 吴军. 数学之美[M]. 北京:人民邮电出版社,2020:275-277.

(收稿日期:2023-06-07 编辑:余迪)

Research on the Ubiquitous Form of Digital Identity and Its Ethical Risk Governance/ZHANG Feng, YANG Li(School of Marxism, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: Digital identity exists in a digitized form, coexisting with cyberspace. The ubiquitous nature of the internet, omnipresent at all times, presents digital identities in forms such as cloud-based, micro-based, hypertext-based, visualized, and fragmented. While enhancing convenience in human life and production, it also entails certain ethical risks. The unreasonable application of digital identity primarily targets four ethical issues: identity, privacy, freedom, and justice. Specifically, it manifests as the weakening of personal and societal identity, leading to a dilemma in integrative privacy protection and the privacy paradox. It obscures individuals' free will and societal ability to forget, implying issues of data bias and unjust algorithmic logic. With the increasing prevalence of the internet, traditional identities are gradually transitioning towards digital identities, making the enhancement of ethical risk governance related to digital identities a crucial topic of our time. In this new developmental phase, there should be a comprehensive utilization of collaborative interactions among technology, law, and ethics to achieve the coordinated governance of ethical risks associated with digital identity. This involves enhancing the sense of digital social identity, safeguarding digital identity privacy rights, overcoming the alienation of digital identity, mitigating the discriminatory impacts of algorithmic logic, enabling it to better serve socio-political-economic development, and meeting the aspirations for a better life among people. From a technological governance perspective, there is a need to reinforce technological innovation and development while overcoming the inherent negative effects of technology. On the legal governance front, it is crucial to uphold the legislative principle of balancing rights and obligations, providing legal safeguards for digital identity applications. From an ethical governance standpoint, all stakeholders must strengthen self-restraint and consciously become an essential complementary force in the governance of digital identity.

Key words: digital identity; ubiquitous form; ethical risk; collaborative governance