

特色专题

构建人工智能隐私治理的伦理责任共同体

潘建红, 杨珊珊

摘要 人工智能技术的广泛应用引发了隐私泄露风险、隐私保护、隐私治理等困境。要解决人工智能隐私困境,需要不同主体共同参与,构建由政府引导,科学家、企业、社会组织、媒体、社会公众等多元主体共同参与的伦理责任共同体。伦理责任共同体具有共同的利益诉求、价值共识、伦理基础和愿景目标,是利益、责任和价值的有机统一体。通过满足各责任主体利益诉求,形成伦理责任主体价值共识,推进伦理责任主体共治模式,实现人工智能隐私困境的善治。

关键词 人工智能;隐私困境;伦理责任共同体

习近平总书记指出:“要加强人工智能发展的潜在风险研判和防范,维护人民利益和国家安全,确保人工智能安全、可靠、可控”^[1]。人工智能技术给人类生活带来诸多便捷,同时也加剧了人类隐私侵犯风险的产生。面对人工智能带来的隐私困境,应如何治理,社会各主体在治理中需要承担怎样的责任,以及如何构建多元共治的伦理责任共同体,成为当前社会关注的焦点。

1 人工智能技术引发的隐私困境

人类已经步入由人工智能技术催生的数字化、智能化、信息化时代,解决人工智能时代下的隐私困境问题,探索良性互动的治理路径,成为必须要面对的现实。当前,数据、算法与算力成为人工智能技术发展的重要部分,也构成了探索人工智能隐私困境治理的主线。其中,数据是人工智能技术开展的首要要素。大数据的大体量、高速度输入输出和多样性

特征,渗透到人类社会的方方面面,极大地方便了人类的生活,提高了社会运转效率。但是,在涉及到数据收集、处理、应用的每一个环节,都有潜在的个人数据泄露风险和过度分析利用,造成隐私保护困境和隐私治理困境。“随着人类文明的发展,……在精炼文化的影响下,公民更容易被暴露于众,因此他们更加需要独处和隐私”^[2]。阿伦·威斯汀^[3]提出了一种新型信息隐私权:隐私是个人、群体或机构自主决定在何时以何种方式在多大程度上将有关自身的信息披露给他人的权利。普罗瑟将隐私权侵权行为归纳为侵犯隐私或独处、对私生活的宣传或公开揭露他人私生活事实、公开丑化他人形象,以及盗用姓名或肖像等4种类型^[2]。我国的《民法典》指出,隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息^[4]。由此可知,隐私权是个人所拥有的一种不为他人知晓、不向社会公开、不受外界所扰的权利。

传统社会通过血缘、地缘、亲缘相联系,个人的信息大多数是公开的,只有极少数的个人信息和生活成为隐私。进入现代社会后,人与人之间成为靠

北京科技大学马克思主义学院,北京 100083

收稿日期:2023-12-05;修回日期:2024-09-30

基金项目:教育部高校思想政治理论课教师研究专项重大课题攻关项目(22JDSZKZ03);北京市习近平新时代中国特色社会主义思想研究中心重大项目(24LL-ZXA096);教育部人文社会科学研究青年基金项目(21YJC720017)

作者简介:潘建红,教授,研究方向为科技管理、科技哲学、马克思主义理论,电子信箱:Pan177@163.com;杨珊珊,博士研究生,研究方向为马克思主义理论,电子信箱:735898163@qq.com

引用格式:潘建红,杨珊珊.构建人工智能隐私治理的伦理责任共同体[J].科技导报,2025,43(4):30-36;doi:10.3981/j.issn.1000-7857.2023.12.01859

经济和工作联系的陌生人。在陌生人社会,人们很少关心别人的信息,个人信息也很少被公开,个人隐私与信息公开保持着平衡关系。在人工智能时代,技术的发展使得个人信息被获取的途径更为多元,获取方式更为智能,获取手段更为隐秘,获取程度更为广泛。这一时期,数据成为重要的资源,数据带来的利润,使利益相关者为了追求利益最大化而侵犯他人的隐私,个人的信息越来越公开透明,容易陷入隐私困境。

1.1 隐私泄露风险

第一,个人信息被过度收集。数据获取是数据积累的过程,人工智能时代数据获取的途径多样。人们使用的各类软件应用程序,如支付软件、通信软件等,在安装使用过程中,为了可以使用相关的产品,必须让渡部分隐私权利,同意软件授权的内容,如“需要访问你的通讯录”“获取你的地理位置”“打开麦克风权限”等信息,尽管这些软件以格式条款的形式征得了用户的授权同意,进而读取、收集、存储用户的信息。但是极易出现用户的个人信息被过度收集。这些被过度收集的数据信息,一旦被泄露或者被别有用心之人窃取、批露、恶意倒卖,将会引发各类社会问题。轻则用户受到商家推销短信、广告电话的骚扰,重则利用用户的个人身份信息对其实施电信诈骗。而随着生物识别技术的发展,除了个人的姓名、性别、年龄、地址等信息外,人脸、指纹、声音等也成为被窃取的对象,甚至能够利用“AI换脸”达到诈骗目的。人工智能时代,数据的收集、分析、应用通常不是由同一类型的公司运营,而海量的数据要在不同类型的公司中间储存和传输,甚至经过数据经纪人的倒卖,在这种情况下,个人的“知情同意原则”往往发生嬗变。

第二,个人状态与行为被预测。算法作为人工智能技术的核心驱动力,在数据获取的基础上,通过对数据进行挖掘和分析,能够判断和预测用户的行为和习惯,分析用户的潜在需求,精准推送相关内容,影响用户的行为选择。例如,商家通过挖掘分析用户的喜好、行程、习惯等历史数据,通过数据之间的关联性为用户画像,利用算法推荐给用户推送相关产品,投放广告,进而影响用户的购物行为,以此获取商业利润,甚至出现大数据“杀熟”现象。智能

手机无所不在的大数据监听,通过监听获取用户的对话信息,分析用户需求,利用各类软件为用户精准投放广告。可以说,在人工智能时代,人类面临的隐私困境并不仅仅局限于隐私数据的泄露,还体现在大数据对人类状态和行为的预测上^[5]。米歇尔·福柯^[6]曾提出过“全景监狱”的比喻,人工智能时代由数据、算法、算力构成的大数据将个人隐私全方位地暴露于公共空间之中,个人的一举一动完全处于被监控状态,形成了所谓的“超级全景监狱”,处于其间的人成为毫无隐私可言的“透明人”。

第三,人的主体性丧失。首先,算法推荐在一定程度上限制了个人的选择方向,将用户困于“信息茧房”之中,用户对于人工智能的依赖加剧,用户的选择权被限制,用户的自由意志被侵犯。其次,在一个文明社会,隐私权作为个人拥有的一种基本道德权利,应该受到尊重和保护。而人工智能带来的隐私风险,直接将人的隐私置于公共视野之中,这是对个人人格尊严的践踏。最后,在人工智能时代,个人的身份信息处于高度透明化状态,通过各类数据信息就能完全拼出一个人的画像,了解一个人的行为习惯、喜好特征。人成为数据的表征,不是主体想把自身塑造成什么样的人,而是客观的数据来显示主体是什么样的人^[7]。这在一定程度上造成人的主体性地位的丧失。

1.2 隐私保护困境

人工智能时代,数据获取的手段更为隐秘,数据获取的途径更为多元,内容更为广泛,这就使得个人隐私保护成为一大困境。首先,隐私侵权的主体很难判定。传统隐私侵权的主体大多是可被判定的个人,但是人工智能时代个人的隐私泄露可能发生在数据收集获取、传播、分析和应用的各个环节,用户往往难以证明侵犯隐私的主体到底是谁,隐私信息是被恶意倒卖还是由于技术设计缺陷被泄露。其次,用户被侵权的过程和隐私泄露的内容也无从感知,即使用户发现隐私泄露,但是具体泄露时间、泄露的信息内容用户也很难知道,这给隐私保护带来了很大困难。最后,用户在面对由于隐私泄露而引发的一系列伤害,如算法歧视、商家大数据杀熟甚至诈骗时,很难获得救助。

1.3 隐私治理困境

人工智能时代,数据成为利益相关者追逐的对象。通过对数据的大量获取,可以获取巨额的利润,在庞大的利益面前,往往造成了追求利益最大化而侵犯他人利益。由于人工智能涉及到多方利益,利益相关者之间的冲突如何化解,利益如何分配,成为人工智能隐私治理的困境。首先,多方利益相关者之间的冲突。人工智能时代个人的利益是在获取技术便利的基础上保障隐私安全,而公共利益是指政府部门通过收集大量的数据进而实现社会治理。企业商业利益与社会责任的冲突,企业如何在追求商业利益最大化过程中承担起相应的责任,个人利益与公共利益之间如何达成平衡是人工智能隐私困境治理的关键。其次,在隐私治理中,个人隐私与更重大的公共利益之间的平衡意味着个人需要让渡部分隐私权,但是在具体的实践中,存在着隐私让渡边界模糊,管理不规范,用户对隐私让渡的范围边界、隐私泄露风险的认知不同,导致隐私治理也会存在差异。

2 人工智能隐私困境治理的伦理责任共同体的生成与实践

要解决人工智能隐私困境问题,单纯依靠政府的力量是不够的,需要社会群体、个体共同参与,形成合力,合理划分人工智能隐私困境治理的伦理责任,协调利益关系,明确责任边界,构建由政府引导,科学家、企业、社会组织、媒体、社会公众等多元主体共同参与的伦理责任共同体,共同应对人工智能带来的隐私困境。

2.1 人工智能隐私困境治理的伦理责任共同体生成逻辑

齐格蒙特·鲍曼^[8]认为,共同体是“社会中存在的、基于主观上或客观上的共同特征(这些共同特征包括种族、观念、地位、遭遇、任务、身份等)(或相似性)而组成的各种层次的团体、组织”。为了解决人工智能的隐私困境,需要构建伦理责任共同体。伦理责任共同体基于成员共同的利益诉求,具有共同的价值目标,通过成员的共同参与、协商、合作,达到价值层面的统一,形成价值共识,提升成员之间的相互依存性与凝聚力,着

力于人工智能隐私困境治理的责任承担,致力于成员共同愿景目标的实现。伦理责任共同体具有共同的利益诉求、愿景目标、价值准则,也是利益、责任和价值的有机统一体。

第一,共同的利益诉求是伦理责任共同体构建的核心纽带。人工智能隐私困境的治理围绕着伦理责任共同体的利益协调展开。马克思指出,“没有共同的利益,也就不会有统一的目的,更谈不上统一的行动”^[9]。共同的利益是伦理责任共同体形成的基础,也是构筑共同体内部秩序与关系的前提。数据的挖掘和应用是造成人工智能隐私困境的直接原因,更深层次的原因在于数据挖掘与应用中社会各主体以自身利益为重,进而侵犯其他主体的利益,其中就包括隐私权。因此,各主体利益的多样性,以及利益之间的矛盾和冲突是导致人工智能隐私困境的源头。在伦理责任共同体的叙事语境中,必然要利益相关者共同参与,寻求共同体中公共利益的最大化,通过沟通、对话、协商使各主体利益分配之间达到平衡,处理好个人利益与公共利益之间的关系,实现利益共享。

第二,价值共识是伦理责任共同体构建的思想根基。伦理责任共同体是价值共识生成的场域。在隐私困境治理中,各主体通过共同协商、共同决策,达到在关于隐私困境治理思想观念、价值层面、目标层面的趋同和统一,促进各主体之间的信任、理解和认同,在各主体间建立公平、协作、可信赖的信任关系。协调利益矛盾,化解利益冲突,达成价值共识,凝聚伦理责任共同体力量,引导伦理责任共同体的行为选择。如在人工智能技术研发阶段,科学家与企业、公众达成价值共识,在产品的设计时考虑到用户的可接受程度,设计生产出符合各责任主体共同价值的产品,尽可能地降低关于隐私问题带来的冲突^[7]。

第三,共同的道德准则、行为规范构成责任伦理共同体的伦理基础。人是社会存在物,人与人、人与社会之间的关系需一定的道德准则来规范。通过加强伦理责任共同体内部道德准则和行为规范的建设,能够促使提升各主体间的合作效率,为伦理责任共同体的运转提供动力。在人工智能隐私困境治理中,通过共同体的道德准则、行为规范来调控各主体行为,促使多主体间开展对话协商及合作共治。

第四,责任共担是伦理责任共同体构建的要求。人工智能引发的隐私治理困境,涉及到多元复杂的社会关系和多方的利益冲突,容易出现责任主体不明、道德主体不清,问责追责难以操作和难以落实等问题。因此,构建伦理责任共同体的要求就是通过共同的利益、共同的价值目标将各主体联合起来,倡导多主体协同合作,共同承担起自身的责任,使各主体知责明责、守责担责、履责尽责,实现风险共抗,责任共担,利益共享,增强伦理责任共同体的凝聚力,形成强大的治理合力,提升人工智能隐私困境的治理效能,实现人工智能隐私困境的善治愿景。

2.2 人工智能隐私困境治理的伦理责任共同体责任划分

第一,政府要加强人工智能隐私风险的监管。人工智能时代,大数据技术的应用极大提高了政府治理的效能,数据成为推动社会发展的重要资源。但是数据被过度读取和使用也容易造成隐私泄露风险。为构建良性运转、健康发展的社会环境,政府需要从顶层设计着手,加强制度建设,强化对人工智能技术应用和隐私风险的监管力度。推动人工智能隐私安全相关立法的完善和修订,制定相关的制度和管理条例,严格规范数据收集、使用者的行为,避免隐私泄露、隐私被过度分析利用情况的产生,对人工智能从研发到应用的各个环节做好管理。政府还要做好大数据隐私风险的研判和评估,对人工智能技术应用阶段所涉及的隐私风险做到事前预防,事中管控,事后处理。确保公民的隐私权利不被侵犯,保障社会隐私安全。

第二,科学家要强化伦理道德教育,弘扬科学家精神。科学家作为人工智能技术的研发者,需不需要承担伦理责任,需要承担怎样的责任,是一个值得探讨的问题。约纳斯认为承担责任有3个必要条件。(1)行为对社会产生影响;(2)行为受行为主体的控制;(3)行为主体可以预见行为产生的后果。对照此3个必要条件,可以看出科学家对人工智能引发的隐私困境需要承担相应的责任^[10]。科学家作为人工智能技术研发的主体,其科研行为受自身控制,在一定程度上还能够研判隐私数据泄露的风险。1968年,波普尔^[11]在《科学家的道德责任》演说中指出,“智慧本身就意味着责任:是在知识上的预见创造了责

任。”人工智能时代,科学家的科研行为、道德选择等都会对技术处理流程产生深远的影响。例如,在一些算法中蕴含了设计者的价值取向和道德取向,存在着“算法黑箱”现象,从某种程度上来说,算法设计者道德选择的不确定性加剧了算法歧视的可能。因此,在人工智能隐私困境治理中,科学家承担着不可推卸的伦理道德责任。科学家要形成伦理责任自觉,提升自身的道德修养,弘扬科学家精神,从技术研发的源头减少隐私侵犯风险发生的可能。

第三,企业要实现利益获取与承担社会责任的平衡。近年来,欧美国家提出了“负责任创新”理念,所谓“负责任创新”就是将科技伦理、企业社会责任和创新有机结合起来,从责任、伦理视角共同应对技术引发的风险^[12]。企业作为市场的主体,通过对用户数据信息的采集、挖掘、分析获取商业利益。在人工智能时代,企业除了追求利益最大化外,还要承担相应的社会责任,积极参与应对人工智能时代由数据收集、分析、应用引发的隐私风险挑战。首先,在技术手段层面,企业要不断推动数据保护技术创新,破解技术风险,推动隐私计算技术的发展,保障数据在流通和融合中的“可用不可见”,避免因技术问题造成用户隐私的泄露^[13]。其次,加强企业员工的职业伦理道德教育,避免员工因个人获利而出现恶意倒卖、窃取用户信息的行为。最后,可在相关企业内部设立人工智能治理专业委员会,对人工智能涉及的隐私问题,做好行业内部管理和规范,强化行业自律,合理合法使用数据,不过度收集用户信息,科学评估数据收集、分析中的隐私泄露风险,研判新技术发展带来的隐私风险挑战,实现利益获取与承担社会责任的平衡。

第四,社会组织要倡导行业自律。社会组织作为区别于政府和企业的主体,在人工智能隐私困境治理中担负着促进行业自律、监督行业行为、推动社会智库建设、倡导政策法律伦理等责任^[14]。一方面,社会组织能够积极推动解决人工智能隐私困境问题相关政策、法律法规的建设,为人工智能隐私困境治理建言献策,提供智力资源,推动相关智库建设。另一方面,在人工智能技术的应用阶段,社会组织能够针对数据收集、存储、处理、使用等各环节,推动建立人工智能隐私保护行业内部规范,制定行业内部标

准,并在全行业内部推广实行,成为全行业遵守的规范准则。与法律制度相比,行业内部规范是一种行业内部的自我约束,在一定程度上更强调道德约束。同时,社会组织还能发挥监管的作用,对于人工智能技术可能涉及到的隐私问题做好防范监管,倡导行业自律,对于违反伦理道德,侵犯个人隐私的行为,实行行业内部的驱逐。

第五,媒体要做好人工智能隐私安全的监督。为解决人工智能带来的隐私困境,需要对人工智能技术的研发者和数据的收集、使用者做好监督。除政府监管、社会组织、公众监督之外,媒体在人工智能隐私问题的监督方面作用不容小觑。相对于其他主体的监督,媒体监督的覆盖面更广。媒体通过对商家、企业侵犯用户隐私问题的报道、揭露和抨击,及时曝光、反映各类侵犯用户隐私的行为,在社会上引发广泛关注,进而推动隐私侵犯问题的解决。同时,媒体还要在社会层面做好人工智能时代隐私安全的宣传和引导,提升公众的隐私泄露防范意识。

第六,要培养社会公众与人工智能时代相匹配的隐私素养。社会公众既是人工智能技术的受益者,也是隐私泄露的受害者,更是隐私困境治理的参与者和监督者。一方面,社会公众要提升自我防范意识,认识到隐私保护的重要性,培养与人工智能时代相匹配的隐私素养。对于过度收集、读取用户信息的行为有明确判断,做好人工智能时代隐私安全的监督者,在各类软件使用中,一旦发现隐私泄露或者隐私被过度读取问题,社会公众要能够及时向相关部门反映,情况严重的要用法律手段保护自己的隐私权。另一方面,要提升自己的伦理道德修养,尊重他人隐私,不利用技术手段侵犯他人隐私,共同维护人工智能隐私安全。

2.3 人工智能隐私困境治理实践

当前,关于人工智能隐私困境的治理国内外进行了相关实践探索,通过制定发展规划、管理办法、立法、发布行政命令等手段,对人工智能引发的数据安全问题进行治理,形成了关于人工智能隐私困境治理的多样化的举措。通过梳理人工智能隐私困境治理的相关实践,为人工智能隐私困境治理的实践路径和方向提供参考借鉴。《国务院关于印发新一代人工智能发展规划的通知》指出:“加快推动无人驾

驶、服务机器人等细分应用领域的行业协会和联盟制定相关标准”^[15]。强调了在人工智能隐私困境治理中行业协会可以发挥重要作用。《互联网信息服务算法推荐管理规定》要求:“参与算法推荐服务安全评估和监督检查的相关机构和人员对在履行职责中知悉的个人隐私、个人信息和商业秘密应当依法予以保密,不得泄露或者非法向他人提供”^[16]。对涉及到用户隐私泄露的环节进行了规范。《中华人民共和国个人信息保护法》要求“任何组织、个人不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息”^[17]。从法律层面保障个人隐私不被泄露。欧盟、美国等对于人工智能治理也形成了诸多法案、条例。美国颁布了《关于安全、可靠、值得信赖地开发和人工智能的行政命令》,指出联邦政府将确保数据的收集、使用和保留合法、安全,并降低隐私和保密风险。各机构应使用可用的政策和技术工具,包括适当的隐私增强技术,保护隐私并应对因不当收集和使用个人数据而导致的更广泛的法律和社会风险^[18]。美国斯坦福大学发布了《反思人工智能时代的隐私问题——针对“以数据为中心”世界的政策建议》白皮书,提出了确保数据集在整个生存周期的透明度,要求问责制必须是任何解决数据隐私的监管体系的重点^[19]。欧洲理事会批准通过的《人工智能法案》,该法案明确强调保证隐私权,在处理个人数据时,适用欧盟数据保护法中规定的的数据最小化和数据保护原则^[20]。

3 构建人工智能隐私治理的伦理责任共同体的路径

要解决人工智能隐私困境,需要构建基于共同利益、具有共同价值目标、承担共同责任的伦理责任共同体。在满足各责任主体利益诉求及共同价值导向的引领下,推进伦理责任主体共治模式,实现人工智能隐私困境的善治。

3.1 满足伦理责任主体的利益诉求

马克思指出,“利益把市民社会的成员彼此连接起来”^[21]。人工智能隐私困境治理涵盖多元伦理责任主体,各责任主体要实现协同共治必须协调好利益分配关系,满足各伦理责任主体的利益诉求。伦理

责任共同体也是利益共同体,只有利益协同才能形成治理合力,共担责任,共抗风险。首先,各伦理责任主体有着共同的利益需求,在人工智能时代,各伦理责任主体都在享受人工智能带来的便捷,研发者也是使用者,也面对着共同的隐私侵犯风险。每个主体都是人工智能的受益者,每个主体也都可能陷入人工智能隐私困境。共同参与人工智能隐私困境治理,是维护各伦理责任主体利益的需要。其次,要明确利益相关者各自的利益诉求,统筹协调利益冲突,化解利益矛盾,最终实现各伦理责任主体的利益最大化。例如,企业作为数据的收集者和使用者,其利益诉求是获取商业价值,而社会公众的利益诉求则是在使用智能技术的基础上保护自身隐私不被侵犯。二者作为伦理责任的主体,要满足各自的利益诉求,就需要达到追求经济价值与保护隐私安全的平衡。让包括人工智能技术研发设计者、使用者、监督者在内的各伦理责任主体都能享受人工智能带来的便捷,而不是陷入隐私困境之中。

3.2 形成伦理责任主体价值共识

人工智能时代,无论是技术研发的科学家,算法设计的工程师,还是收集数据的企业商家,亦或是使用各类智能软件的个人,无不是人工智能运行环节的参与者。发挥伦理责任共同体的作用,实现人工智能隐私困境的共治,需要在伦理责任共同体内部达成价值共识,形成共同的价值目标。价值共识是指不同价值主体之间通过相互沟通而就某种价值或某类价值及其合理性达成一致意见^[22]。伦理责任共同体也是价值共同体,各伦理责任主体达成价值共识,能够消解不同价值取向带来的冲突,减少在人工智能隐私困境治理中涉及的利益矛盾,提高隐私困境的治理效率。首先,构建伦理责任共同体的第一核心要义是负责。各责任主体在实践中要明确自身责任,增强合作意识,建立互相信任、互相包容、协商共治的参与机制,使各伦理责任主体最大化发挥作用,共同应对人工智能时代下的隐私风险。其次,各伦理责任主体要强化行为自律。伦理责任主体既是人工智能隐私困境的治理者,也承担人工智能的研发、推广及使用责任。在治理中各责任主体要增强自律意识,在监督规范人工智能隐私困境治理时,也要做好自身约束,通过共同的价值引领实现人工智

能隐私困境的共治。

3.3 推进伦理责任主体的协同共治模式

人工智能隐私困境治理强调伦理责任各主体的协同参与。各伦理责任主体要综合运用法律制度、伦理规范和技术手段,实现人工智能隐私困境治理的现代化。协同治理是对于多元治理主体关系的重塑,强调主体之间的多元协同合作关系,以及组织使命的一致性,通过跨界合作解决单一组织难以有效治理的公共问题^[23]。人工智能隐私困境协同共治模式是为了更好地发挥多方力量作用,实现各伦理责任主体优势互补,良性互动。首先,伦理责任共同体要形成共同的人工智能隐私困境治理目标和愿景,遵循负责、公平、包容、开放、协作的治理原则,搭建多元主体共同参与、共享信息的平台,保持各主体之间的协作性,激发各主体间彼此合作的意愿。其次,伦理责任共同体通过举办各类论坛、沙龙、会议,将科学家、企业、社会组织、媒体和社会公众等代表聚集在一起,共同探讨人工智能隐私困境的治理对策,实现不同主体之间的协商、交流与合作,推动建立人工智能隐私困境治理生态系统。最后,要加强伦理责任共同体内部组织机制、运行机制和激励机制的建设,保障各伦理责任主体能够遵守共同体内的行为准则和规范,保障伦理责任共同体的良性运行,充分调动各伦理责任主体参与伦理治理的积极性,提升人工智能隐私困境治理的效能。

人工智能造成隐私困境的很大原因在于利益相关者之间的利益冲突和矛盾,探索人工智能隐私困境的治理主线,要推动构建人工智能隐私困境治理伦理责任共同体,实现多主体参与、责任共担、利益共享。

参考文献 (References)

- [1] 加强领导做好规划明确任务夯实基础 推动我国新一代人工智能健康发展[N]. 人民日报, 2018-11-01(001).
- [2] 张民安, 林泰松. 隐私权的界定[M]. 广州: 中山大学出版社, 2017.
- [3] Westin A F. Privacy and freedom[M]. New York: IG Publishing, 1967: 1.
- [4] 中华人民共和国民法典[EB/OL]. (2020-06-01) [2024-09-05]. <https://www.chinacourt.org/law/detail/2020/06/id/150163>.

- shtml.
- [5] 王强芬. 大数据时代背景下医疗隐私保护的伦理困境及实现途径[J]. 中国医学伦理学, 2016, 29(4): 685-689.
- [6] 米歇尔·福柯. 规训与惩罚: 监狱的诞生[M]. 刘北成, 杨远婴, 译. 北京: 生活·读书·新知三联书店, 2012: 219-256.
- [7] 薛孚, 陈红兵. 大数据隐私伦理问题探究[J]. 自然辩证法研究, 2015, 31(2): 44-48.
- [8] 齐格蒙特·鲍曼. 共同体: 在一个不确定的世界中寻找安全[M]. 欧阳景根, 译. 南京: 江苏人民出版社, 2003: 1.
- [9] 马克思恩格斯文集(第二卷)[M]. 北京: 人民出版社, 2009: 359.
- [10] Jonas H. The imperative of responsibility: In search of an ethics for the technological age[M]. Chicago: The University of Chicago Press, 1984: 90.
- [11] 卡尔·波普尔. 走向进化的知识论[M]. 李本正, 范景中, 译. 杭州: 中国美术学院出版社, 2001: 11.
- [12] 王前, 菲利普·布瑞. 负责任创新的理论与实践[M]. 北京: 科学出版社, 2019.
- [13] 隐私计算联盟. 隐私计算白皮书[EB/OL]. [2024-09-05]. <http://221.179.172.81/images/20221229/48421672279200206.pdf>.
- [14] 刘红春. 人工智能社会组织监管的合规型路径[J]. 天津法学, 2021, 37(2): 37-44.
- [15] 关于印发新一代人工智能发展规划的通知[EB/OL]. (2017-07-20) [2024-09-05]. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
- [16] 互联网信息服务算法推荐管理规定[EB/OL]. (2022-01-04) [2024-09-05]. https://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.
- [17] 中华人民共和国个人信息保护法[EB/OL]. (2021-08-20) [2024-09-05]. https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.
- [18] The White House. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence [EB/OL]. (2023-10-30) [2024-09-05]. <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/>.
- [19] King J, Meinhardt C. Rethinking privacy in the AI era: Policy provocations for a data-centric world[R/OL]. (2024-02-22) [2024-09-05]. <https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world>.
- [20] European Parliament. Corrigendum[R/OL]. (2024-04-19) [2024-09-05]. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf.
- [21] 马克思恩格斯全集(第二卷)[M]. 北京: 人民出版社, 1957: 154.
- [22] 汪信砚. 普世价值·价值认同·价值共识: 当前我国价值论研究中三个重要概念辨析[J]. 学术研究, 2009(11): 5-10.
- [23] 袁静, 刘晓媛, 臧国全. 用户参与共治: 政府开放数据隐私风险治理的新思路[J]. 图书情报知识, 2022, 39(6): 101-112.

Construct a community of ethical responsibility for the privacy governance of artificial intelligence

PAN Jianhong, YANG Shanshan

School of Marxism Studies, University of Science and Technology Beijing, Beijing 100083, China

Abstract The wide application of artificial intelligence technology has led to difficulties such as privacy leakage risk, privacy protections, and privacy governance. To solve the dilemma of artificial intelligence privacy, a government-led ethical responsibility community should be constructed involving multiple subjects participation, including scientists, enterprises, social organizations, media and the public. Ethical responsibility community is an organic unity of interest, responsibility and value, with common interests, value consensus, ethical foundation and vision goals. By satisfying the interests of all responsible subjects, the value consensus of ethical responsible subjects is formed, and the co-governance model of ethical responsible subjects is promoted to achieve good governance of the privacy dilemma of artificial intelligence.

Keywords artificial intelligence; privacy dilemmas; ethical responsibility community ●



(责任编辑 卫夏雯)