医疗人工智能背景下隐私权保护研究

陶金婷 袁紫藤 程美琦 杜芸路 郑雅琪 陶 瑜 陶沐可 田永谦 张宇清

（湖北中医药大学人文学院 武汉 430065）

〔摘要〕 介绍医疗人工智能背景下隐私权特征和内容，阐述国内外隐私权保护法律规制现状，分析医疗人工智能背景下隐私权保护所面临的挑战，提出贯彻隐私权保护原则、明确隐私权保护内容、完善监管体系等对策。

〔关键词〕 医疗；人工智能；隐私权保护

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2020.05.003

Study on Privacy Protection in the Background of Medical Artificial Intelligence *TAO Jinting, YUAN Ziteng, CHENG Meiqi, DU Yunlu, ZHENG Yaqi, TAO Yu, TAO Muke, TIAN Yongqian, ZHANG Yuqing, Humanities College of Hubei University of Traditional Chinese Medicine, Wuhan 430065, China*

〔**Abstract**〕 The paper introduces the characteristics and contents of privacy right in the background of medical Artificial Intelligence (AI), expounds on the status quo of domestic and foreign privacy protection laws and regulations, analyzes the challenges faced by privacy protection in the background of medical AI, proposes to implement the principles of privacy protection, clarify the content of privacy protection, improve the regulatory system and other countermeasures.

〔**Keywords**〕 medical; Artificial Intelligence (AI); privacy protection

1 引言

随着人工智能技术飞速发展，广泛应用在医疗机器人、影像识别、智能诊断、医疗数据统计、健康管理等领域，提高医疗水平、降低医疗成本、给公众带来极大便利，但同时也给隐私权保护带来前所未有的巨大挑战。隐私权是自然人享有的对其个人、与公共利益无关的个人信息、私人活动和私有领域进行支配的一种人格权。医疗人工智能应用场景中需要通过交易、交换和转移等多种形式，使数据为多人所使用，而这种共享又必须以收集、存储和利用部分公民的隐私为必要条件。在人工智能时代直面因技术发展而带来的隐私权保护问题，探讨如何有力保障隐私权是必要且迫切的。

2 医疗人工智能背景下隐私权特征及内容

2.1 特征

2.1.1 主体权利有限让渡性 隐私权的有限让渡是指权利主体基于对相关主体的信任，为实现健康诊疗目的在一段时间内让渡部分隐私给相关主体。例如在权利人与医疗机构的权利让渡过程中，患者必须主动向医务人员提供既往病史、曾服用药物、症状等并允许其监测个人医疗信息；相对而言，医务人员也必须了解到患者真实、详细的健康状况和

〔修回日期〕 2020－05－26

〔作者简介〕 陶金婷，本科生，发表论文2 篇；通讯作者：张宇清，硕士，讲师，发表论文20 余篇。

疾病阶段，才能给出正确合理的医嘱。在权利人与智能健康管理平台之间的权利让渡过程中，权利人需要不断将个人健康数据传输至健康平台，从而获取个人健康记录和信息分析数据。

2.1.2 隐私数据精确性 包括正确性和精准性。医疗人工智能背景下隐私采集方式可来自于临床医疗机构及其实验数据以及智能可穿戴设备等，特殊的隐私采集方式保证其正确性，采集内容主要包括但不限于患者病历中的详细记载，病情、个人史、家族史、接触史、身体隐私部位、异常生理物征等病理和个人生活秘密，这些隐私数据可以精准定位到个人。例如每个人的基因信息是独一无二的，利用基因信息可定位到信息主体。

2.1.3 权利救济高难度性 人工智能时代，隐私内容一旦泄露不可逆转。当医疗隐私数据流入人工智能系统，各数据端口相互连接，信息传送速度快、范围广，使得权利主体无法及时切断其传送路径。隐私数据会在各个接收者之间流转，根据特定场景需求被多向度、多层面地聚合，隐私主体难以对流动的数据进行修正或删除，损害结果不可逆转且有可能不定期反复。与此同时权利人的举证证明较为困难，无法有力保障自身权利。

2.1.4 侵权行为隐匿性 机器学习需要利用信息完善其功能，这要靠数据驱动，无法在黑暗中运行[1]。据2019 年《华尔街日报》报道谷歌在美国21 个州秘密收集数百万份患者病历数据，包括实验室结果、医生诊断、住院记录、患者完整健康历史及其姓名和出生日期，这一计划被称为“夜莺计划”，医生和患者对该计划都不知情。权利主体往往只是表示同意采集，其隐私信息被隐秘地在不同端口传递，被记录留底，即使最后知晓自身隐私已经被不法泄露，众多情况下甚至不知道何时何地何人实施了侵权行为。

2.2 内容

2.2.1 占有权 指自然人以自主意愿管领和控制自身隐私的法律可能性。隐私占有权是其他相关隐私权利的基础，其他权利是隐私占有权的相关衍生。在医疗人工智能背景下，自然人的医疗隐私可能被医务人员、健康数据处理平台、医疗信息共享平台等同时占有，但需明确这种“占有”应当是有时效性的，其主动权应当由权利主体把控。

2.2.2 支配权 指自然人依法依照个人意愿对其隐私享有使用、利用和处分的权利。例如自然人将个人健康数据交由健康管理平台分析，患者同意人工智能根据病理切片等辅助诊断其所患疾病，这些都是权利主体对隐私实行支配权的表现。但需注意，对于自身隐私的使用、利用和处理不得违反法律的强制性规定以及公序良俗，也就是民法上的“禁止权利滥用原则”。

2.2.3 保密权 在医疗人工智能领域，医疗机构或智能设备在获取患者或用户个人隐私后应当履行严格的保密义务，包括权利人的个人信息、生活状况、基因信息等一切权利主体不愿意公开的个人事项。医疗机构以及医疗人工智能设备的相关平台在没有法律、行政法规的明确规定或者未经权利主体明确表示同意的情形下不得以任何形式向社会公众或其他个人提供权利主体的隐私信息。

2.2.4 利益维护权 指权利主体对于个人隐私所享有的维护其不可侵犯性、在受到非法侵害时可以寻求司法保护的权利。在医疗人工智能领域，患者和用户有权对其隐私进行保密以保证其隐私权不受侵犯，包括：禁止医疗机构或设备平台非法收集患者或用户信息资料，传播其个人资讯；对于除患者或用户同意外的一切私人活动，禁止医疗机构或设备平台进行干涉、追查、跟踪、拍照、录影等非法搅扰行为；对于私有领域，如身体状况、通信信息等，禁止医疗机构或设备平台通过医疗人工智能进行偷看和宣扬，禁止未经权利人允许在医疗人工智能内安装窃听、监视装置等。

3 人工智能时代我国隐私权保护立法现状

3.1 宪法

我国的根本大法，第38、39、40 条分别规定公民的人格尊严不受侵犯、公民的住宅不受侵犯、公民的通信自由和通信秘密受法律保护。

3.2 民事法律法规（表1）

表1 民事法律法规

施行日期	法律名称	法律条目	法律位阶
1988. 4. 2	最高人民法院关于贯彻执行《民法通则》若干意见	第160 条	法律
2010. 7. 1	《侵权责任法》	第2 条 第62 条	法律
2017. 10. 1	《民法总则》	第110 条	法律

3.3 刑事法律法规（表2）

表2 刑事法律法规

施行日期	法律名称	法律条目	法律位阶
2017. 11. 4	《刑法（修正案十）》	第245 条；第252 条；第253 条	法律

3.4 行政法律法规（表3）

表3 行政法律法规

施行日期	法律名称	法律条目	法律位阶
2004. 1. 1	《乡村医生从业管理条例》	第24 条第3 项	行政法规
2008. 5. 2	《护士条例》	第18 条；第31 条第3 项	行政法规
2009. 10. 1	《流动人口计划生育工作条例》	第18 条	行政法规
2017. 7. 1	《残疾预防和残疾人康复条例》	第21 条第2 款	行政法规
2017. 12. 1	《志愿服务条例》	第21 条；第36 条	行政法规
2018. 10. 1	《医疗纠纷预防和处理条例》	第42 条；第50 条第4 项	行政法规
2017. 9. 1	《行政处罚法》（2017 修正）	第42 条第3 项	法律
2019. 5. 15	《中华人民共和国政府信息公开条例》	第50 条	行政法规
2019. 7. 1	《中华人民共和国人类遗传资源管理条例》	第9 条第2 款；第12 条第1 款	行政法规

3.5 其他法律法规（表4）

表4 其他法律法规

施行日期	法律名称	法律条目	法律位阶
1992. 10. 1	《妇女权益保障法》	第42 条第1 款	法律
1999. 5. 1	《执业医师法》	第22 条第3、9 项	法律
2004. 12. 1	《传染病防治法》	第12 条第1 款；第68 条第5 项；第69 条第7 项	法律
2007. 6. 1	《未成年人保护法》	第39 条；第69 条	法律
2017. 6. 1	《网络安全法》	第12 条第2 款；第45 条	法律
2009. 1. 1	《电子商务法》	第25 条；第87 条	法律
2020. 6. 1	《基本医疗卫生与健康促进法》	第33 条	法律

目前正在提交第13 届全国人大审议的《中华人民共和国民法典（草案）》将人格权单独成编，对隐私权和个人信息保护设置专章，明确规定自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人隐私权。草案还首次对隐私进行明确界定：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、活动、信息。隐私权是人格尊严的核心，是一个人社会人格的关

键。隐私一旦遭到侵害具有不可逆的特点，《民法典（草案）》体现了对隐私的周全保护。

4 人工智能时代域外隐私权保护法律规制

4.1 美国

保护公民隐私的体系较为完整。人工智能在医疗领域应用中需要积累大量数据，要实现数据积累就要打破各个医院和社区之间的壁垒。为此美国建设电子健康记录系统（Electronic Health Records，EHRs），在 10 年内积累 1 000 万名患者信息。美国较早注意保护个人隐私，逐渐将医疗健康信息归入隐私权保护范围内。美国 1974 年通过《隐私权法案》（The Privacy Act）；1996 年针对不同权利主体进行隐私数据信息技术保护等，接着通过《健康保险携带与责任法》（Health Insurance Portability and Accountability Act，HIPAA），在随后几年中不断对法案进行修正及补充，最终于 2003 年正式生效。HIPAA 要求各机构必须采取适当措施保护权利主体信息的私密性。此外 HIPAA 中还规定很多对 EHR 的相关隐私保护细则，对使用 EHR 系统也有明确规定，是否可以对 EHR 加以利用取决于信息是如何建立、谁在维护以及当事人情况[2]。对隐私权保护的实际立法情况以及 HIPAA 相关规定反映出美国企业对于公民隐私权形成了一套较为完整的保护体系，可以称为医疗健康数据领域领跑者。

4.2 欧盟

目前世界上对隐私规定最为详细和严格的国际组织，其在医疗人工智能隐私保护方面尤为重视数据隐私的保护，对数据隐私的定义及保护规则全面且严格。自 1970 年起欧盟开始针对隐私数据保护实施统一政策，于 2016 年出台、2018 年正式实施的《通用数据保护条例》（General Data Protection Regulation，GDPR）被称为史上最严数据保护法案。GDPR 以保护欧盟公民个人数据为关键，将其纳入人权组成部分，借助其高额判罚来建立数据保护的高标准。在医疗领域人工智能背景下，GDPR 依然适用于欧盟公民的隐私保护工作。权利主体有权要求数据控制者删除其收集到的个人信息，也可以将个人医疗数据上传至新的数据控制者，这加强了权利主体对其个人信息的控制权与处分权，同时也对医疗人工智能的数据来源起到很好的控制作用。

4.3 英国

在英国医疗服务体系（National Health Service，NHS）医院与 DeepMind 合作的医疗试验初期，NHS 向谷歌 DeepMind 部门提供约 160 万患者的详细资料。该信息用于开发和完善一个诊断和检测系统，用于发现患者是否处于急性肾损伤（Acute Kidney Injury，AKI）风险中。然而英国最高隐私保护监管部门表示这项试验并没有告知患者医疗记录数据的使用方式。此后英国迅速加强在医疗人工智能隐私保护方面的研究，虽然起步较晚但逐渐形成系统化法律体系。自 1998 年的《数据保护法案》以来，英国先后发布《信息自由法》、《开放数据白皮书：释放数据潜力》、《公共部门信息再利用条例》，数据隐私保护逐渐从私人领域扩展到公共领域[3]，此外为推动隐私数据立法还专门建立信息专员办公室。可以看出英国在医疗人工智能隐私权保护方面的研究将沿着数据隐私保护的方向进行拓展，结合其政府对于医疗人工智能隐私保护的重视程度，未来在该领域具有广阔前景。

4.4 日本

由于数据、技术和商业需求较为分散，难以系统地发展人工智能技术和产业，所以其有关医疗人工智能隐私权保护的法律是比较零散且不完善的。代表性较强的是 2005 年开始实施的《个人信息保护法》。值得关注的是日本专门建立匿名加工制度，即对个人隐私数据进行匿名加工后便无法识别出具体个人信息，规定这些信息虽来源于个人，但加工后并不属于个人，具有公共属性，匿名加工信息的使用不需要获得个人同意。可见日本在隐私权保护方面较他国相比更为新颖，在今后医疗人工智能领域下的隐私权保护中以匿名加工这一制度为基础，逐步完善相关法律，将使隐私权得到行之有效的保护。

5 医疗人工智能背景下隐私权保护面临的挑战

5.1 隐私数据采集和使用存在安全隐患

医疗人工智能快速发展和广泛应用会产生大量数据，涉及个人敏感信息和核心隐私。例如人工智能通过各大医院云共享技术和大数据平台记录每位用户信息，存储用户自使用设备时起的所有医疗记录、基因、遗传信息等敏感隐私数据。通过强大的数据整合和分析能力，人工智能甚至可以推算出用户未来健康状况及其家族潜在的基因信息。另外医疗人工智能设备在采集用户隐私信息时，如果某用户端缺少隐私保护措施，那么第 3 方也可能在传输过程中截获传输的数据，窃取蕴含用户隐私的行为数据。

5.2 隐私权主体知情同意权难以实现

权利主体的知情同意是传统隐私权保护中的重要准则，信息收集主体应在自身合法性的基础上，在获得当事人同意的前提下收集信息并在法定的或当事人同意使用的范围内使用信息[4]。在医疗人工智能时代，大数据的信息合成和传播对权利主体的知情同意权带来巨大挑战。首先，信息收集主体其合法性无从考证，在医疗人工智能中各信息端口相互连接，系统获取的个人隐私等数据信息会传送至各个端口，而分支端口连接其他信息网络，导致个人数据传输迅速且无法确保每个端口获取行为的合法性。其次，隐私权主体与医疗人工智能设备数据收集主体之间不对等，包括数据占有体量、数据处理能力、数据传递渠道的不对称等[5]。这会导致隐私权主体一方面无法完全了解系统运作模式，另一方面无法选择测量隐私数据和生理机能范围和程度。该设备一旦使用，用户隐私数据的最终流向不在权利人控制范围内，使隐私权主体行使知情同意权时力不从心。最后，医疗人工智能数据收集方、处理方以及分析方通常都不是同一人或同一方。例如医疗机构对收集的数据进行采样分析进而传送到下一环节，再由下一环节人员进行其他对比分析，依次推进。用户隐私信息会通过医疗设备进行多次传送，无法测量知晓用户个人隐私的群体，用户无法行使其知情同意权。

5.3 算法黑箱和举证责任冲突

算法黑箱是指由于技术本身的复杂性以及媒体机构、技术公司的排他性商业政策，用户并不清楚算法的目标和意图，也无从获悉算法设计者、实际控制者以及机器生成内容的责任归属等信息，无法对其进行评判和监督。例如智能可穿戴设备，用户全天候提供自身健康信息，平台反馈健康分析，而用户只得到平台的分析结果，不知晓其分析依据、数据处理是否正确、科学。根据《侵权责任法》第 63 条规定，医疗机构及其工作人员侵犯隐私权采过错责任为归责原则。第 36 条规定网络用户、网络服务提供者利用网络侵害他人民事权益采过错责任为归责原则。根据“谁主张，谁举证”举证证明责任一般规则，被告方需证明侵权责任的 4 个构成要件，即使其能够举证侵权行为、损害结果及主观过错，但对于因果关系的论证往往会陷入算法黑箱的难题。可见算法黑箱加剧了侵权者和受害者角色的不平衡和受害人举证责任的困难，人工智能信息处理、传输系统具有高度的自主性和灰色性，即使是设计者、开发者、生产者也很难解释其中的缘由，受害者就更难证明行为和事实之间的因果关系，维权更加艰难。

6 医疗人工智能背景下加强隐私权保护的对策

6.1 贯彻保护原则

6.1.1 合法收集 指法律、法规授权的机构收集有关用户或患者隐私信息时，必须依据相关法律法规，明确告知权利主体其收集信息的目的和用途，权利主体对是否提供信息、信息使用目的和方式有决定权。收集个人资料应取得个人明示同意后才可进行。医疗机构收集有关信息时，要通报所收集内容，若收集内容与其所提供的内容不符，被收集人有权拒绝提供信息。

6.1.2 最小限度 指法律、法规授权的机构在收集个人隐私信息时，原则上应只收集其需要的部分

信息，如果只需要收集个人普通信息即可实现，不应该收集信息主体个人敏感信息。同时法律、法规授权的机构在收集个人相关隐私信息时应保证收集过程秘密性，防止隐私内容被第3方知晓，造成隐私泄露。

6.1.3 限制使用 指除非权利人同意，法律、法规授权的机构不得以除涉及社会公共利益需要和国家政治利益需要之外的任何理由公开、使用、传播个人隐私等。例如医疗机构不能向第3方提供患者隐私信息，也不应以研究为理由与其他医疗机构共享隐私信息。

6.1.4 安全保护 指法律、法规授权的机构对其收集和掌握的个人信息应采取必要的管理和技术防护措施，以免个人信息被盗取、泄露、丢失[6]。例如医疗机构除最基本的加密措施外，还应安排医疗机构相关技术人员周期性地对收集的个人隐私数据进行审核，建立高强度的监督体系，严密监察个人隐私数据，最大限度地防止个人隐私泄露风险。

6.2 明确保护内容

6.2.1 权利主体享有的权利 综合我国目前对于隐私权的保护现状以及借鉴欧盟的《通用数据保护条例》，隐私权权利主体至少应享有以下权利：一是知情权，数据控制者从权利或其他来源处收集医疗信息时应提供对等的信息，以确保数据主体对其自身权利以及救济途径的充分知晓。二是被遗忘权，当出现收集和处理数据已不再必要、权利主体撤销同意、权利主体行使拒绝权、医疗隐私数据被非法处理等情形时，权利主体有权要求控制者立即删除相关信息，数据控制者应采取合理措施并告知正在处理该个人数据的其他控制者。三是拒绝权，数据主体有权基于自身情况拒绝包括直销目的以及公众或第3方利益在内的医疗隐私数据处理行为。

6.2.2 隐私权客体范围 传统意义上的隐私权客体范围较窄，主要包括私人空间及信息，如姓名、年龄、籍贯、性别、财产状况、婚姻状况、健康状况等。随着互联网及人工智能的发展，个人信息因财产属性增强，越来越多的内容需要被列入隐私权保护的客体。正在提交全国人大审议的《民法典（草案）》人格权编中规定，隐私包括私密空间、信息和活动。随着医疗人工智能的快速发展，较为适当的方法是采取概括加列举的方式及时补充相应客体内容来适应新时代、新技术的法治需要。

6.3 完善监管体系

6.3.1 形成行业自律规范 目前人工智能行业有以下3种自律规范：一是建议性行业指引，大多由保护个人隐私的自律组织共同制定行业指导性规则，参加该组织的成员需承诺遵守此规则。二是网络隐私认证计划，通过对达到个人隐私保护相关标准的医疗信息处理机构颁发隐私认证的方式，督促相关机构促进对个人隐私的保护。三是技术保护方式，根据不同平台网页交互时所需要的用户信息对其分门别类，用户可根据隐私偏好设定隐私阈值，若平台项目采集超出该设定范围的信息阈值，则会自动向用户发出警告。针对医疗人工智能这一特殊领域，还应加入医疗机构、互联网平台或从事数据处理的企业人员的行业自律规范，加强人员管理和培训，使其充分认识到保护患者或用户隐私的重要性，恪守行业规范。

6.3.2 建立第3方监管机构 对于人工智能产业的专业化、技术化特点，可借鉴域外经验，建立专门的第3方监管机构，减少因分散监管导致的监管空白。首先，医疗人工智能的专业化要求监管机构具有相应专业技术能力和设备支撑，同时因为领域的特殊性，监管机构还需要具备医疗研究、法律专业人员；其次，除临床病历等信息，绝大部分的具有隐私性的健康信息实际是由数据企业掌握，政府公权力的过度放松会使其不正当使用公民隐私从而获取收益，而过度介入则会打压企业创新技术的积极性，因此如何在两者之间找到平衡点需要逐步摸索；最后，第3方监管机构的设立应有一整套侵权责任法律体系，以保障机构的监管措施落到实处。

6.3.3 提升人工智能系统可追溯性 主要是指设计、生产人员应在设计、生产人工智能系统的过程中注重涉及可追责性和可验证性方面的计算机科学制度。这一制度可类比我国食品安全管理制度，覆

（下转第37 页）

20 刘娟，郑君君，吴江. 在线医疗网站患者选择医生的影响因素实证研究［J］. 医学信息学杂志，2017，38（5）：48－51.
21 邓朝华，洪紫映. 在线医疗健康服务医患信任影响因素实证研究［J］. 管理科学，2017，30（1）：43－52.
22 胡蓉，陈惠芳，徐卫国. 移动医疗服务中医患互动对患者感知价值的影响－－以知识共享为中介变量［J］. 管理科学，2018，31（3）：75－85.
23 李娟娟，周宁丽. 即时通讯（IM）实时咨询应用研究［J］. 图书情报工作，2009，53（13）：97－99，37.
24 史磊. 医患会话特征研究［D］. 长春：吉林大学，2007.
25 李战子，陆丹云. 多模态符号学：理论基础，研究途径与发展前景［J］. 外语研究，2012（2）：1－8.
26 Blei D M，Ng A Y，Jordan M I. Latent Dirichlet Allocation［J］. Journal of Machine Learning Research，2003（3）：993－1022.
27 魏慜慧，董洁，魏磊. 门诊医疗会话特征－－中国大学校医院与三甲医院的比较［J］. 南京医科大学学报（社会科学版），2014（6）：456－460.
28 耿敬北，陈子娟. 网络社区多模态话语分析－－以 QQ 群话语为例［J］. 外语教学，2016，37（3）：35－39.
29 Roter D L，Larson S，Sands D Z，et al. Can E－mail Messages between Patients and Physicians be Patient－centered?［J］. Health Communication，2008，23（1）：80－86.
30 Hogan T P，Luger T M，Volkman J E，et al. Patient Centeredness in Electronic Communication：evaluation of patient－to－health care team secure messaging［J］. Journal of Medical Internet Research，2018，20（3）：e82.
31 吴孝仙. 某三甲医院孕妇网络健康信息搜寻行为调查［J］. 中华医学图书情报杂志，2018，27（5）：61－64.
32 Holtz B，Smock A，Reyes－Gastelum D. Connected Motherhood：social support for moms and moms－to－be on Facebook［J］. Telemedicine and e－Health，2015，21（5）：415－421.
33 Gui Xinning，Chen Yu，Kou Y，et al. Investigating Support Seeking from Peers for Pregnancy in Online Health Communities［J］. Proceedings of the ACM on Human－Computer Interaction，2017，1（CSCW）：50.
34 Sillence E，Hardy C，Briggs P. Why Dont We Trust Health Websites That Help Us Help Each Other?：an analysis of online peer－to－peer healthcare［C］. Paris：Proceedings of the 5th Annual ACM Web Science Conference，2013：396－404.

（上接第 23 页）

盖人工智能原材料工厂、生产加工企业、销售终端、使用人员等整个企业链条的上下游，通过专用硬件设备进行信息共享，最终服务于智能医疗的消费者。一旦在消费者端出现任何问题，可以通过人工智能标签上的溯源码进行查询，明确事故方相应责任。

7 结语

随着 5G 技术成熟和发展，人工智能与医疗将不断深入融合，给公众带来更多便利，人们的隐私权保护意识也随着技术的进步而不断加强。但是智能技术的发展依靠数据，必然会带来隐私权被侵害的风险。法律制度具有滞后性，但关于法律问题的思考应该是前瞻的。针对医疗人工智能应用场景中新出现的数据安全与隐私保护等问题，需要在政府、企业、民间机构、公众密切合作基础上，努力削弱不利影响，创建人类与人工智能彼此信任的未来[7]。

参考文献

1 刘春杰. 谷歌的人工智能战略 仍难越过隐私这道坎［J］. 计算机与网络，2016，42（21）：19.
2 王旭. 大数据医疗时代的人工智能与隐私保护［J］. 电子产品世界，2019，26（6）：79－81.
3 栾轶玫，鲁妮. 人工智能时代国际传播中的数据隐私保护［J］. 国际传播，2019（3）：8－20.
4 张新宝. 信息技术的发展与隐私权保护［J］. 法制与社会发展，1996（5）：16－25.
5 许天颖. 人工智能时代的隐私困境与救济路径［J］. 西南民族大学学报（人文社科版），2018，39（6）：166－170.
6 时诚. 重大疫情防控中个人信息的法律保护［J］. 中国矿业大学学报（社会科学版），2020，22（2）：63－74.
7 许天颖. 人工智能时代的隐私困境与救济路径［J］. 西南民族大学学报（人文社科版），2018，39（6）：166－170.