

doi: 10.15936/j.cnki.1008-3758.2018.03.002

# 家庭泛用型智能机器人的安全风险研究

阎国华, 闫晨

(中国矿业大学 马克思主义学院, 江苏 徐州 221116)

**摘 要:** 伴随着人工智能的兴起, 泛用型智能机器人正在快速发展, 逐步走进寻常家庭。鉴于强大的功能预设, 家庭泛用型智能机器人往往需要收集家庭信息、介入家庭生活甚至扮演家庭角色, 使其为家庭生活带来便利的同时也可能引发信息隐私、生命财产、道德伦理等安全风险。这些风险有任何产品因其工具性而产生的常规风险, 也有机器人功能定位带来的特色风险, 还有机器人智能性而引发的成长风险。因此, 在肯定家庭泛用型智能机器人技术优势的同时, 还应从增强信息安全、促进本质安全和关注人机和谐等视角, 多措并举, 力图消除或降低其潜在安全风险。

**关 键 词:** 智能机器人; 家庭泛用型; 人工智能; 安全风险; 伦理

**中图分类号:** N 031

**文献标志码:** A

**文章编号:** 1008-3758(2018)03-0227-06

## On the Security Risks of Universal Home-used Intelligent Robots

YAN Guo-hua, YAN Chen

(Marxism School, China University of Mining and Technology, Xuzhou 221116, China)

**Abstract:** With the rise of artificial intelligence, universal intelligent robots are rapidly developing and gradually entering ordinary households. In view of their powerful presupposition, universal intelligent robots often need to collect family information, intervene in family life or even play a family role to bring convenience to family life and may also lead to security risks of information privacy, life and property, and moral ethics. These risks include the conventional risks of any product due to its instrumentality, the distinctive risks posed by the functional positioning of robots, and the growth risks associated with robot intelligence. Therefore, in affirming the advantages of smart home-used intelligent robot technology, every effort should be made to eliminate or reduce its potential security risks by enhancing information security, promoting intrinsic safety and paying attention to human-computer harmony.

**Key words:** intelligent robot; universal home-used; artificial intelligence; security risk; ethics

人工智能研究由来已久, 当下已初步进入应用阶段。借助于仿生材料、人工视觉、机械制造、语言合成与识别等学科的同步发展, 人工智能的应用领域日渐广泛, 在日常生活领域的突出应用当属家庭智能机器人。目前, 家庭智能机器人种

类繁多, 涵盖医疗陪护、儿童看护及家用清洁等功能, 且尚有更多种类处于开发之中。这些家庭智能机器人有的定位于单一功能, 如地面清洁; 也有的具备多种功能甚至提供用户自开发功能, 属于泛用型智能机器人。后者也是本文的主要研究对

收稿日期: 2018-01-11

基金项目: 教育部人文社会科学研究资助项目(17JDSZ1020); 国家社会科学基金资助项目(17BZX037)。

作者简介: 阎国华(1977-), 男, 河北邢台人, 中国矿业大学教授, 管理学博士, 主要从事技术哲学、思想政治教育研究。

象。因为功能强大,类人化趋势不断提升,家庭泛用型智能机器人会深度介入家庭生活,为家庭生活提供便利,但也常常引发安全风险。这些安全风险可能涉及到隐私信息泄露、生命财产安全及伦理与道德秩序调整等方方面面。本着扬长避短、未雨绸缪的精神,有必要在家庭泛用型智能机器人大规模进入普通家庭之前对这一问题开展深入研究,找出其安全风险的表现形式、诱发风险的内在机制和消除风险的改善策略。

## 一、家庭泛用型智能机器人安全风险评估

基于目前应用和未来功能预期,家庭泛用型智能机器人会日渐深入地参与家庭工作、扮演家庭角色,以及介入家庭生活。从参与到扮演再到介入是一个不断加深的过程,家庭泛用型智能机器人可以带来生活便利,但其特殊工作模式也可能在信息安全、生命财产和伦理道德等领域引发安全风险。

### 1. 信息隐私安全风险

基于机器学习和智能体理论,家庭泛用型智能机器人在日常工作中需要收集家庭信息并进行智能化处理,从而完成对家庭环境和自身行为的预设判断<sup>[1]</sup>。收集信息的行为本身并不直接引发风险,但全信息化信息收集和信息长期累积势必会让机器人逐渐积累和贮存大量家庭内部信息。这些信息被集中电子化贮存既方便机器人工作,也存在着两个方面的数据安全风险:①海量家庭信息电子化贮存的稳定性问题。依靠卷积神经网络实现世界抽象表征的深度学习是机器人的工作基础。收集信息、分析数据是提高机器人自身智能化程度的基本需求<sup>[2]</sup>。为了满足泛用性工作职能,家庭泛用型智能机器人的信息收集往往非常全面,甚至是不加选择进行全信息化收集。这些信息可能包括家庭成员信息、家庭位置信息、家庭生活模式信息,其中以家庭成员信息尤为敏感。同时,信息收集形式也往往细腻而全面,可能包括声音、图像、视频等多种形式。海量家庭信息被持续性、高细腻度、累积性地收集和电子化贮存本身就存在安全风险,因为一旦机器人出现突发系统紊乱或遭遇病毒攻击极易出现信息主动与被动泄露问题。②全信息化信息收集诱发目的性窃取。家庭泛用型智能机器人的信息收集质量很高,且具有

持续性、全信息化等突出优点。这些信息有些属于非敏感信息,有些则可能是覆盖个人金融数据、健康状况和商业机密的敏感与隐私信息。敏感与隐私信息可能会创造极高的经济价值,也常常因此为非法窃取提供了目的因与动力因,对个人隐私安全构成威胁。例如,金融信息被窃取可能造成个人财产损失。同时,批量泄露的数据可能会被进行再处理,在现代大数据技术的帮助之下,有可能用于呈现更加深层的相关性联系而非因果性联系,所提取出的强相关结论可能威胁使用泛用型智能机器人家庭的正常生活秩序<sup>[3]</sup>。

### 2. 生命财产安全风险

家庭泛用型智能机器人能够为家庭提供的服务及帮助日益增加,工作能力日益增强,但其强大的活动能力是一把“双刃剑”,在为家庭服务的同时也对家庭生命财产安全构成潜在威胁。潜在生命财产安全风险的诱发因素既包括本质风险、操作风险,还包括外界风险。具体主要有:①系统功能突发紊乱。技术发展往往存在阶段性和技术极限。任何智能电子产品都无法实现绝对稳定和可靠。系统功能突发紊乱使得机器人行为安全性无法绝对保障,给用户正常生活带来概率极低但却无法完全消弭的不确定风险。例如,因系统故障给所看护的病人重复喂药,后果不堪设想。②系统遭遇非法劫持。机器人运行常常需要网络支持。因此,沿着网络途径,家庭泛用型智能机器人可能会被非法分子部分或整体劫持。在遭遇劫持的情况下,机器人运行存在多种安全隐患。诸如,机器人的监控系统能够成为犯罪分子的“第三只眼睛”,帮助他们窥探家庭实时状况从而为犯罪行为提供动机或时机;机器人被远程控制成为直接“帮凶”,在家庭内实施破坏行为;机器人协助他人实施犯罪行为,如打开家庭门锁、关闭家庭安全保护装置,等等。③用户存在越界使用。智能机器人功能的稳定性和准确性注定会存在边界。在超过边界运行的情况下,系统功能的稳定性、可靠性乃至安全性将会急剧下降。因此,如果用户对机器人的功能边界掌控模糊,对机器人使用可能越界的指令,而机器人又没有拒绝的情况下,可能会导致机器人自身或其他物品损坏。

### 3. 伦理道德安全风险

家庭泛用型智能机器人具有与环境交互的能力,当它与人类近距离共同生活时,往往会扮演一定的家庭角色,因此被赋予社会伦理属性<sup>[4]</sup>。在

“人一机”亲密交互过程中,被人类深度赋能的智能机器人不断提升自身力量和自主程度,而其不断提升的智能性和家庭介入感显著相关。家庭角色的获取势必会引发其与家庭成员的关系问题,不当的人机关系处理会诱发伦理道德风险<sup>[5]</sup>。因此,在购买机器人时,主人不仅需要做物质上的付出,还要做好精神和心理上的准备,注意应对几种可能的伦理道德风险:①角色定位中的关系处理。智能机器人会成为我们的奴隶、伙伴、家人还是主人是一个急迫的问题。根据融入程度不同,智能机器人会获取不同家庭角色<sup>[6]</sup>。机器人的角色定位由其功能发挥所决定,如果浅层介入就是家用工具,如果深度介入则成为家庭成员。深度介入的机器人会引发两个方面的人机关系风险:其一,人机相互信任。人机信任机制有可能顺势等同于人与人之间的信任机制,但基于程序运行的机器人随时处在被攻击篡改的危险之中,容易诱发信任风险<sup>[7]</sup>。其二,人机情感依赖。深度生活介入会帮助机器人获得家庭成员地位,引发人对机器人的情感付出,产生情感依赖。同时,将机器人从“家用工具”提升为“家庭成员”还可能引发后续淘汰机器人时需要面对的善后处理风险。②接纳过程中的心理调适。智能机器人参与家庭生活,可能会使用户心理上产生被机器人“监控”的不适感。如果不能适应机器人的“注视”,将有可能引发用户的负面情绪,使其产生压抑、尴尬等不适,进而扰乱正常生活秩序<sup>[8]</sup>。此外,购买“进口机器人”可能因文化差异产生道德风险<sup>[9]</sup>。③沟通过程中的情感交流。机器人在运行过程中将无可避免出现“犯错”情况。部分家庭泛用型智能机器人具有模拟人类情感功能,如果不能帮助它分辨正确、错误及最恰当的行为,机器人实际运行可能会出现情绪化、盲目化、机械化问题,存在反智能性风险。同时,由于机器学习,如何为机器人创造良好的家庭学习参照系,避免交流缺失与不当引导使智能机器人“性情”顽劣,扰乱正常生活秩序也是需要警惕的潜在风险<sup>[10]</sup>。

## 二、家庭泛用型智能机器人风险成因

上述可知,家庭泛用型智能机器人在实际运行过程中可能诱发各种风险。这些风险的成因来自不同层面,有任何产品因其工具性而产生的常

规风险和机器人功能定位带来的特色风险,还有机器人智能性引发的成长风险。

### 1. 由于工具属性引发的常规风险

任何一件器物在作为工具出现时,都可能因为自身可靠性、应用规范性、操作正确性等因素诱发风险。家庭泛用型智能机器人首先是一种工具,因此也难以摆脱应用时的常规风险。对于由工具属性决定的常规风险,可从机器人自身主体和外界环境两方面考察。①自身可靠性无法完全保证。可靠性是保证安全性的重要条件,但可靠性又往往是相对的,没有绝对的可靠,因此也就没有绝对的安全。机器人也是一样,其系统和功能设计不能确保没有缺陷。越是复杂的系统,可靠性越难以保证。硬件配置缺陷和软件设计缺陷都可能会导致机器人在实际工作中无法完全达到预定目标与外界期望<sup>[11]</sup>。这种情况下,如果使用者或机器人缺乏警惕,则可能会产生安全风险。②操作正确性无法完全保证。电子产品的智能性很多源于对特定工作的批处理程序,但批处理程序在高效的同时,也让一项命令承担了更多的使命感。从这个意义上讲,机器人智能性越高,人类操控便捷性越好,对人操作正确性的要求也会随之提高,因为错误操作、违规操作、越界操作等都会在机器人的实际运行中诱发不确定性风险<sup>[12]</sup>。③意外状况无法完全避免。除了机器人本身可靠性和使用者操作正确性之外,可能对安全形成挑战的还包括意外状况的发生。作业场地的限制、外界因素的干扰等问题也会使得机器人面临不确定性风险。例如,机器人对工作温度、湿度、光线强度、目标可辨识度等方面也有很高要求。

### 2. 由于功能定位引发的特色风险

不同于一般性工具,依靠独特的工作原理,机器人有着相对独特的功能设定,也因此会引发一些特色风险。基于家庭泛用型智能机器人的功能定位,其特色风险来源主要有:①个体环境的千差万别性。机器人在销售之前虽力图在多种环境测试,但还是难以摆脱有限环境参数的限制,存在面临情况无限性和预设情况有限性的矛盾。在进入消费者家中之后,由于家庭环境迥异,机器人不仅功能发挥受到影响,还可能会遇到不可知的风险。②人机动作转换的复杂性。人类一些习惯性动作,轻而易举可以完成的动作,在机器人完成时往往要分解成很多步骤,涉及多个关键技术。每个环节的准确性,环节间的衔接可靠性都将影响整



个工作完成的质量和安。例如,人可以轻松取来的茶杯,换做机器人去取,则需要视觉识别、准确定位、机械抓取等环节的协同工作。因此,每一个动作就像一个系统,动作越复杂,系统的边界周长越大,可靠性也越差。③难以完全消除的机械性。智能机器人“类人”但“非人”,难以根本消除的“机械性”限定了它还无法像人一样灵活处理问题。一边是机器人的“墨守成规”、程式化和固定化,一边是日常家庭生活存在随机性和多样性需求,二者之间的矛盾短期难以消除。④客户需求的无限性。对于机器人,每个家庭、个人或单位,往往有不同的需求,而机器人的研发者很难根据每一种特定需求开发出相应的应用。尤其对于泛用型智能机器人,功能边界的有限性和客户需求的无限性之间往往存在分歧。

### 3. 由于智能属性引发的成长风险

智能性无疑是家庭泛用型智能机器人最炫目的名片,但“智能性”是把“双刃剑”,给机器人带来学习功能、应变功能和发展功能的同时,也引发了相关的成长性风险。成长风险主要是指因为机器人功能成长而引发的风险问题,而功能成长主要依靠的就是智能性。由智能属性诱发的机器人成长风险主要来源其自我决策、自我判断与自我成长的质量:①自我决策的不稳定性。智能性赋予机器人自我运算能力,使其可以通过对已收集信息的处理实现一定程度上的自我决策。但是,数据的有限性、运算程序的先进性都决定了机器人自我决策能力的有限性<sup>[13]</sup>。因此,机器人有限的决策能力和无限的实际情况之间常常存在尖锐的矛盾。这种矛盾决定着自我决策质量,而低决策质量的自我尝试可能会导致机器人引发相应风险。②自我判断的不准确性。与智能机器人功能存在有限性边界不同,外界对机器人的期望存在无限性需求。有限性与无限性的冲突可能引发用户“超范围”使用风险。当用户下达的指令超过既定功能边界,机器人的自我判断能力就变得非常重要。然而在目前,机器人对自身能力的自我判断往往还不够准确,一味地执行用户命令可能导致自身受损或伤及用户。另一方面,机械本质决定智能机器人理解的僵化性难以彻底消除,还不能像人一样对指令进行透彻理解,为使用过程增加了很多不确定性。③自我成长的不确定性。由于具有机器学习功能,机器人一定会对周围所处环境进行适应和学习。家庭泛用型智能机器人的

自我成长是处在变化中的存在,所处家庭环境的多样性让其自我成长也具有不确定性。在学习过程中,家庭环境可能为机器人提供正确、近乎正确、完全正确及不正确的参考原型。参考原型的不确定性可能让机器人的自我成长面临不确定性。由于机器人具有可塑性特质,因此在不同家庭环境下成长的机器人思想与行为模式可能存在较大偏差<sup>[14]</sup>。例如,在和谐家庭内实现自我成长的机器人可能会比暴力家庭的机器人更加温和,反之亦然。

## 三、家庭泛用型智能机器人安全风险应对策略

上述分析可见,家庭泛用型智能机器人使用过程存在着诸多风险,并不能简单等同于使用非智能电子设备。不过,我们应该努力去应对科技发展可能带来的风险,而不是简单限制或阻止技术的进步<sup>[15]</sup>。目前投入使用的家庭泛用型智能机器人属于人工智能技术初级阶段的产品,未来被人类深度赋能的智能机器人所引发的安全风险将更加严峻。然而,不管形势多么严峻,家庭泛用型智能机器人引发安全风险的底层逻辑是相对稳固的,也正因如此,我们可以就其引发的主要安全风险从以下几个方面来加以应对。

### 1. 创新信息收集与管理,增加信息安全

信息收集是支撑智能机器人工作的基础,但信息泛收集和长时间累积性储存也的确存在巨大的信息安全风险。因此,对于信息泄露引发的安全风险必须从技术角度进行规避。就智能机器人的信息收集与应用机理来看,在不降低机器人智能特性的前提下,可以考虑实施以下几种方式来增强信息安全:①增强脱敏技术强度,隐蔽重要个人信息。通过技术创新,家庭泛用型智能机器人可以实现信息收集与处理同步进行,通过脱敏处理,隐匿重要私人信息,让信息不再具有私密性,很难产生经济价值,从而使信息窃取与信息滥用失去必要条件,进而有效应对因信息泄露引发的安全风险。②引入关键词筛选制,减少盲目收集数量。由于泛收集,家庭泛用型智能机器人运行中可能会收集许多跟自身无关、无用的信息。盲目收集的信息被储存在机器人系统内,既造成存储空间资源浪费,又给想要窃取信息的人以目的因和可趁之机。如果将机器人所需要的支撑数据

建立索引,引入关键信息筛选,可以减少信息收集总量,从一定程度上降低对个人隐私的干预程度及信息泄露的可能性。③定期擦除过期数据,防止人为窃取利用。对于所收集的时间久远且重复使用可能性极小的数据可以进行定期删除,既能彻底抹除数据中虽经脱敏仍存留的信息,也可以降低被人为窃取后借助大数据处理技术提取深层关联结果,对用户造成生活困扰或威胁的机会。

## 2. 增强系统设计与防范,探索本质安全

基于程序运行的机器人随时可能成为被攻击篡改的对象。为最大程度降低机器人成为“帮凶”的可能性,我们可以在其系统中增添预防意外机制、安全保护机制等安全机制。在受到外界非法入侵时,家庭泛用型智能机器人可以进入安全模式、脱机状态或休眠状态等自我闭锁程序,实现阻碍非法犯罪行为、避免问题扩大和减少用户损失的目的。为了实现这一目标,主要可以考虑如下几个途径:①建立可远程控制的超级管理模式,防范意外风险。人的随机性具有比机器人的机械性更加灵活的应变能力。建立可远程控制的超级管理模式,可以在突发意外时对机器人实施终极性控制。例如,对处于被“绑架”状态的机器人下达超级指令。②定时更新防范机制,主动提升系统安全性。追求机器人功能性的同时,需要巩固其安全性。家庭泛用型智能机器人的使用年限相对较长,需要对其进行长期管理,不断更新系统,提升防御能力,从系统受到攻击后被动修复漏洞,转变为主动更新系统防范,降低相关风险产生率。此外,还可以增加安全缓冲区,如闭锁装置和联动装置,来防止误碰风险。③探索安全标准,打造机器人本质安全。本质安全是指通过设计等手段使生产设备或系统本身具有安全性,即使在误操作或发生故障的情况下也不会造成事故的功能。机器人的安全使用一方面是避免系统问题或被劫持,更为重要的是实现家庭泛用型智能机器人的本质安全。这一领域,国际标准化组织已经作出了一些探索,出台了关于“机器人和机器人装置—协同工业机器人”的 ISO/TS15066 技术规范,提出了安全相关受监控停止、手动控制、速度和距离监控,以及压强和力度限制等四个方面的主要指标。同时,德国科学家正在开发一种人工神经系统,教机器人感受疼痛并作出反应,目的是帮助机器人避免其系统遭到损坏,从而避免意外的发生。汉诺威莱布尼兹大学的萨米·哈达丁(Sami

Haddadin)教授所开展的“触觉机器人”研究就是其中的突出代表。除此之外,在用户没有及时回应时,机器人可以进行自主选择脱机状态或自我闭锁等<sup>[16]</sup>。这些努力都指向了一个更高的机器人安全标准,即本质安全型智能机器人。

## 3. 加强产品完善与售后,引导人机和谐

在研发过程中加入机器伦理思想能够引导用户与机器人的家庭相处模式,促进人机交流,为智能机器人创造更利于其工作的环境,从而为用户提供更优质的服务。家庭泛用型智能机器人在家庭的理想角色定位、交流模式、隐私规避等方面都应完善设计,避免用户盲目使用机器人所引发的伦理道德风险。基于对产品属性和售后服务制度地思考,主要的完善措施包括:①增添人情情景思考,改进可能引发尴尬的功能设计。在机器人设计过程中,应当增添实际生活情景的思考,引入关系理论<sup>[17]</sup>。在研发过程中,设计师应尽可能设想和梳理可能引发用户产生不适感、尴尬感的情景,并帮助机器人在投入使用后能自觉并且巧妙地避开这些场景,最大程度给予用户原本的私有空间,缓解智能化产品带来的相关风险。人情情景思考不仅要考虑机器人应用的技术条件,还需要思考机器人应用的不同文化背景和环境<sup>[18]</sup>。②考察用户体验感受,及时发现和解决问题。预设情景有限性与实际情况无限性使机器人无法实现完全不犯错。机器人偶尔“冒犯”可能并不会使用户反感,但如果不及时调整行为模式,长期下去会造成较差的用户体验感,影响机器人的正常使用<sup>[19]</sup>。因此,对于生产方来说,有必要进行定期的考察回访,听取用户建议,及时帮助用户纠正机器人的行为模式,促进人机交流,使用户能够获得适合自己家庭的智能机器人。③完善售后服务制度,实现安全绿色人性回收。鉴于对家庭的全面融入,智能机器人的淘汰问题也往往会引发信息和情感风险。因此,制造商需要承担相应的道德责任和社会责任<sup>[20]</sup>。具体来说,制造商可以通过将定向回收作为家庭泛用型智能机器人售后服务的标准环节,来达到生产与处理的责权利一致。同时,通过专业人员对被淘汰的智能机器人进行信息擦除、整机拆卸、拣选可重复利用硬件及绿色处理废弃元件等,可以实现安全回收、绿色回收、人性回收。

总之,在实际应用中,家庭泛用型智能机器人存在因全信息化信息收集诱发目的性窃取、数据库系统安全难以绝对保障等为突出表现的信息安全

风险,因系统遭遇非法劫持、系统功能突发紊乱、功能边界难以掌握等为突出表现的生命财产安全风险,因角色定位中的关系处理、接纳过程中的心理适应、沟通过程中的情感交流等为突出表现的伦理道德风险。就成因来讲,这些安全风险有因为工具属性诱发的常规风险、因为功能定位诱发的特色风险,以及因为智能属性诱发的成长风险。工具属性诱发风险的原因主要在于功能自身可靠性、工具自身机械性、外界操作正确性、意外状况可能性等;功能定位引发特色风险的主要原因在于个体环境的千差万别性、人机动作转换的复杂性、难以完全消除的机械性和客户需求的无限性;智能属性诱发风险的原因主要在于自我决策质量不可靠、自我判断不准确、自我成长不确定。针对相关安全风险,完善家庭泛用型智能机器人可以从三个方面进行解决:一是创新信息收集与管理,增加信息安全。二是增强系统设计与防范,探索本质安全。三是加强产品完善与售后,引导人机和谐。尽管目前家庭泛用型智能机器人的研发还处于人工智能宏伟蓝图的初级阶段,引发的安全风险可能会日益严峻,但其引发安全风险的底层逻辑相对稳固,使得安全管理并非不可为之。因此,不要因为安全风险去限制和阻止机器人的发展和进入家庭,而是要循着安全风险的产生逻辑,在家庭泛用型智能机器人的设计、开发和应用中不断加以思考和应对,从而最大限度的规避技术缺陷,降低技术风险,保障技术成果优势得以展现。

参考文献:

[1] 林命彬. 哲学视角下智能机器在自我意识和行为意义上的突破[J]. 黑龙江社会科学, 2016(6):8-14.

[2] 龚怡宏. 人工智能是否终将超越人类智能——基于机器学习与人脑认知基本原理的探讨[J]. 人民论坛, 2016(7):12-21.

[3] 维克托·迈尔-舍恩伯格,肯尼思·库克耶. 大数据时代:生活、工作与思维的大变革[M]. 盛杨燕,周涛,译. 杭州:浙江人民出版社, 2013:38.

[4] 杜严勇. 机器伦理刍议[J]. 科学技术哲学研究, 2016,33(1):96-101.

[5] Payr S. Towards Human-robot Interaction Ethics[M]. Berlin: Springer International Publishing, 2015:33.

[6] 李小燕. 从实在论走向关系论:机器人伦理研究的方法论转换[J]. 自然辩证法研究, 2016,32(2):40-44.

[7] 于雪,王前. “机器伦理”思想的价值与局限性[J]. 伦理学研究, 2016(4):109-114.

[8] 李小燕. 老人护理机器人伦理风险探析[J]. 东北大学学报(社会科学版), 2015,17(6):561-566.

[9] 王绍源. 应用伦理学的新兴领域:国外机器人伦理学研究述评[J]. 自然辩证法通讯, 2016,38(4):147-151.

[10] 李俊平. 关于约束人工智能情感的思考[J]. 科协论坛, 2013(1):85-87.

[11] 任晓明,王东浩. 机器人的当代发展及其伦理问题初探[J]. 自然辩证法研究, 2013,29(6):113-118.

[12] 杜严勇. 情侣机器人对婚姻与性伦理的挑战初探[J]. 自然辩证法研究, 2014,30(9):93-98.

[13] Ller V C. Introduction: Philosophy and Theory of Artificial Intelligence[J]. Minds and Machines, 2012,22(2):67-69.

[14] Coeckelbergh M. Moral Appearances: Emotions, Robots, and Human Morality [J]. Ethics & Information Technology, 2010,12(3):235-241.

[15] 约瑟夫·巴科恩,大卫·汉森. 机器人革命:即将到来的机器人时代[M]. 潘俊,译. 北京:机械工业出版社, 2015:214.

[16] Briggs G, Scheutz M. How Robots Can Affect Human Behavior: Investigating the Effects of Robotic Displays of Protest and Distress[J]. International Journal of Social Robotics, 2014,6(3):343-355.

[17] de Graaf M M A. An Ethical Evaluation of Human-Robot Relationships [J]. International Journal of Social Robotics, 2016,8(4):589-598.

[18] MacDorman K F, Cowley S J. Long-term Relationships as a Benchmark for Robot Personhood [C] // IEEE International Symposium on Robot & Human Interactive Communication. Hatfield: IEEE, 2006:378-383

[19] Malle B F. Integrating Robot Ethics and Machine Morality: The Study and Design of Moral Competence in Robots[J]. Ethics & Information Technology, 2015,18(4):1-14.

[20] 周天策. 共处的“中道”——儿童陪护机器人的伦理风险分析[J]. 自然辩证法研究, 2017,33(4):57-62.

(责任编辑:李新根)