人工智能应用的安全风险及法律防控

张 敏 李 倩

摘 要：2017年被称为人工智能元年，AI技术和应用逐步实现突破和落地。人工智能应用在社会各个领域的同时，也带来一系列安全风险。本文从人工智能应用对人类安全的威胁、对社会伦理安全及社会秩序的冲击和对个人生命、数据、隐私等个人安全三个层次进行了安全风险分析，认为应当坚持“人工智能工具论”的法律客体为原则，从自由、限制、禁止应用三个层次对人工智能的应用进行法律规制。

关键词：人工智能应用；安全风险；法律防控；法律人格

中图分类号：D922.29 **文献标识码**：A **文章编号**：1009-2447（2018）03-0108-08

1956年麦卡锡首次提出“人工智能”这一概念，成为人工智能这门新兴学科正式诞生的标志。继21世纪开始进入计算机和互联网时代，到2010年后的大数据时代，到2017年人脑与智能机器人的世纪围棋大战、AlphaGo三连胜击败围棋世界冠军柯洁，再到机器人取代工厂的大量员工，到无人机运送快递、无人驾驶汽车上路，人工智能的应用逐步走进并深入影响人类的工作和生活。基于科学技术的优劣双面性，人工智能应用给社会带来更多便利的同时也相应带来安全风险和隐患，智能水平提升带来颠覆人类安全的潜在风险、智能机器人应用于传统制造业乃至现代服务业打造的智能工厂带来的失业性社会风险、情感机器人应用对社会伦理安全带来的风险，人工智能深度学习所需人类大量数据带来的隐私性风险，人工智能应用导致的风险引发了人类社会的严重关注和热烈讨论。

一、人工智能的核心特征

人工智能又称AI（Artificial Intelligence），是计算机学科的一个分支，又是与控制论、心理学、优生学、自动化乃至哲学密切相关的综合性的学科。其开发主要有三种路径：符号主义学派、连接主义学派、行为主义学派[1]。由于“智能”本身含义就不明确，因此关于人工智能尚未有一个明确的定义。麦卡锡最早对人工智能的定义是“机器可以像人以智能作出行为一样拥有机器智能”[2]。随着技术发展，不同学者对此作出不同的定义，但核心在于模拟“人类智能”，智能指人类所特有的现象和能力，而其他生物不具备的特征。人类智能的表现形式为学习知识、感知现象、理解本质、思维模式，因此可以这样定义智能：智能是人通过观察、理解、思维等来认识事物并通过决策和行为来改变世界和解决问题的能力。《人工智能标准化白皮书》上的定义亦体现了这一核心，人工智能即模拟、延伸人的智能、感知环境和学习知识来解决问题的系统①。虽然定义的描述方式不同，但笔者认为人工智能的本质属性就是模仿人类记忆、感知和学习等活动，达到像人类智能一样对外界反应作出判断并解决问题的目标，总的来说是对人类智能的扩展和延伸。

作者简介：张敏，女，陕西咸阳人，西北工业大学人文与经法学院教授。从事商法研究；李倩，女，山东济南人，西北工业大学人文与经法学院硕士生。从事商法研究。

人工智能之所以叫“智能”是因为深度学习的能力，能够像人类一样识别图像、文字、语言等信息，并通过其算法作出自己的反应。卷积神经网络是模拟人类脑神经网络而创造的“机器”大脑，人工智能深度学习可以像人的视觉，敏锐地观察世界。如今深度学习能力在自动驾驶汽车上的应用能够使汽车更加精准的识别面临的障碍、行人，从而保证驾驶安全；在医学中的应用能够使机器比医生在诊断病情上更加准确。

人工智能在大数据的基础上进行深度学习，这一数据思维源于算法但不依赖于算法，能够随机应变，因此具备一定的创造性思维模式和一定程度的自主性。人工智能不管如何拥有自主决定、推理、运算、创造，但终究不是人脑，也不是人，因为两者的根本区别在于人类拥有复杂的感情和自由意志（Free Will）。自由意志首先是一个哲学概念，是指人们依照其拥有的条件去决定是否做一件事。显然，人工智能根据人们对其特定的设置而在一定程度上拥有自主决策和行为，不可能像人一样可以意识到自我，也不可能像人类一样可以自由选择职业。

人工智能按照智能水平高低可以分为弱人工智能和强人工智能，弱人工智能（Weak-AI）又称初级人工智能，是指人工智能按照输入的特定程序对外界作出反应，进而可以模仿人类的行为，如下棋、语音识别、面部识别等，但是不能作出推理和真正解决问题，也不拥有自我改变和自主意识。强人工智能是指在弱智能基础上的跨越式进步，不是指运算、模仿等能力更加强大的弱人工智能，而是像人一样可以拥有自主意识，成为世界上的主体的智能[3]。强人工智能一是可以像人一样思维，二是超越人的思维模式有独特的思维习惯和行为。如李建中教授认为机器只是看起来有智慧，但是不会像人拥有自主意识一样可以真正的推理和解决问题[4]。邓志东教授认为目前人工智能仍处于感知智能阶段，其视觉识别、自然语言处理、语音识别等方面只是对外界的感知，远远达不到创造性的智能水平[5]。当前人工智能应用的领域越来越广，但都是基于程序设定和深度学习的初级智能，所作出的智能行为依靠大数据，不能够根据情境作出像人一样的智能反应和行为。相当于大脑的强人工智能尚未开发完成，而超越人类大脑的超人工智能还不确定完成时间。

人工智能技术在发展过程中逐步实现了与行业的深度融合，以此来改变传统的生产模式及生活方式。当前学术界和产业界共同推动的产业化阶段认定的发展方向是：制造业、农业、物流、金融、商务、家居、教育、机器人、运载工具、虚拟现实与增强现实[6]。

二、人工智能应用的安全风险分析

安全，从现代汉语的字面上理解是“没有危险，不受威胁，不出事故”。从社会学角度讲，安全是人最基本的需求。在马斯洛提出的人类五个层次的需求中，安全需求处于生理需求之上的第二个层次的需求，安全的需求有对秩序稳定和社会保护的依赖，也有对法律稳定、界限明晰的需求，最基本的需求就是不恐惧、不焦躁、不混乱，所处的环境是可以让人依赖的[7]。安全价值是法的价值中重要内容，一些学者主张将安全提升至法律最高价值之列，以托马斯·霍布斯和杰里米·边沁为代表的法学家早已对安全的概念和价值进行过分析。霍布斯将人民的安全作为政治正义和社会正义的标准和尺度。边沁认为法律最重要的一个目的就是控制社会安全，保护人身和财产安全。博登海默在论述法律的性质和作用时把安全同秩序和正义作了区别和联系。他认为，安全在法律价值中被界定为实质价值，是指实体上真切的感受到安全，没有侵略和侵害，也没有财产的掠夺和不确定的动荡，在生活中不受公害和变故的频繁影响，在健康中不受疾病的困扰而不得治，在生产和工作中不因为年老和失业而失去生活来源，这些都构成了安全的要素[8]。人工智能应用的风险，主要存在于相当于人脑的强人工智能或超越于人脑的超人工智能时代，但随着弱人工智能的普遍应用，也将不断引发人类、社会和个人三个层次的安全问题。

（一）人类安全风险

1.智能自主武器的应用

人工智能技术应用在战争和自主武器以来，对其风险的担忧不亚于对核武器的担忧。军事机器人自投入战场以来在战争中的杀伤力也是逐步提升，且已到达第三代。在美国对外的战争中，人工智能机器人战士杀害了上千名对手的人类士兵，但同时出现了误杀、误伤上百名平民的情况[9]。也有美国对伊拉克战争中出现战地机器人失控而对美方指挥官瞄准、杀害的苗头[10]。

另外，智能武器的发展既有可能导致“人工智能恐怖主义”走向极端。军用机器人发展越发趋向智能化，其独立自主环境探测能力增强。与普通士兵相比其成本更低，杀伤力更大，且伤亡更小。机器人作战更加冷血，不会有恻隐之心，因此引发一场战争更加容易，也有可能会被恐怖组织所利用，形成全球恐怖活动的更高一轮恐慌和破坏。即使是中立的技术，被恐怖组织所利用，会造成更危险的后果，就有可能出现反对论所说的人类灭亡。正如霍金说：“人工智能的全方位发展可能招致人类的灭亡。如最大化使用智能性自主武器[11]。”

2.人工智能应用“失控”的风险

对人工智能失控的担忧根本原因在于所谓“奇点”的到来。人工智能先驱雷·库兹韦尔在他的书中大胆预测，十年后人类大脑可以相互传递信息，二十年后人工智能系统可以植入大脑而形成人机融合体，而三十年后人工智能就会超越人类智能出现可怕的奇点。等到智能水平发展足够高时，我们不能预测人是人工智能辅助的人类，还是有大脑的机器人[12]。中国Mindputer实验室制造出世界首个“人工脑连接体”（True-Brain）的到来使驱雷·库兹韦尔的预言多了几分可能，人工脑指的是对大脑神经结构进行结构性、网络状分析，使机器能够模拟大脑的活动过程，实现人工脑对生物脑活动状态的追踪，到那时与人脑的结构和功能就极其相似，此时出现的就是类脑人工智能超越人类智能的奇点时刻②。正如霍金认为的，人工智能失控实质是对智能发展水平超过人类而成为和人一样的主体，他可以决定自己的复制权和其他需求，而人类失去对其系统的控制，此时人类可能就会被伤害和边缘化，也有可能会被毁灭，甚至颠覆人类。

（二）社会安全风险

1.社会性失业风险

人工智能工作的效率远远高出人类，尤其是在一些重复性、辅助性、制造业等低技术要求的工作领域，人工智能不需要休息也不会抱怨，效率高且精准性也比人类要高的多，此类行业被机器人取代的可能性最大。在劳动密集型行业中，如果劳动者由人工智能取代，失业问题将极其严峻。对于容易被取代而失业的这部分人来说，较快掌握更多机器人所取代不了的技术也是不现实的，因此社会的就业稳定性将大大降低，不安定因素升高。麦肯锡全球研究院发布的报告也对中国人工智能自动化工作即将取代人类约一半的工作内容作出预测，并认为这一可能性在中国极有可能出现[13]。中国智能化带来的失业已经开始上演，银行的裁员③和阿里巴巴启用人工智能员工和客服来取代人类客服、快递员等工作岗位已经有所显现。

人工智能应用取代一些行业既是必然趋势，是当代经济发展中不可阻止和逆转的事实，即使人们会提升自身能力创造其他的就业岗位，但这一过程的速度与人工智能应用发展速度相比显然是缓慢的，个人对社会生产资料分配的需求将在一定时间内得不到满足，失业一旦成为规模必然引起社会秩序的混乱，犯罪率或群体性事件有可能上升，成为威胁社会安全的重大隐患。

2.社会伦理安全挑战

虽然人类与机器的根本区别在于自由意志和人类情感，但机器突破情感限制而拥有情感并不是不可能的，现有研究已有可以感知到人类情绪的陪伴机器人，可以在人类情绪失落时进行安慰。人工智能领域有专家认为人工智能可以获得情感，强人工智能和超人工智能更是具备情感和意志的人类大脑。人类社会是群体性社会，是由人和人之间的关系维系起来的社会，人类需要家人、朋友等的陪伴，情感的交流互通，这是人类的基本需求和人类社会的一般伦理规范。人类的婚姻家庭、工作环境等，都可能会因为机器人拥有感情而使人类孤立，由群居变为独居，社会

结构会发生重大颠覆。可能会发生人和机器人相爱，人面对机器而选择逃避更加复杂、需要付出努力维系的人的关系。具备意志和情感的人工智能将会造成人与人的关系、人与人工智能的关系和人工智能与人工智能的关系更加复杂化和多样化，对人类社会的伦理安全提出重大挑战。

（三）个人安全风险

1.人身损害的安全风险

与其他纯工具性的技术所不同的是，人工智能应用有独立于人的自主学习能力和一定程度脱离人的控制作出智能化决定，及人工智能设计者也不能完全确保人工智能的绝对安全。如中国国际高新技术成果交易会上，应用于教育的“小胖”机器人发生了砸展柜并伤人的事件，2015年德国大众汽车机器人伸手击打工作人员造成死亡的事件，2018年3月美国亚利桑那州优步公司的一辆自动驾驶汽车撞死一名过路行人，成为全球首例自动驾驶汽车撞击行人致死案件，另外用于外科手术的机器人造成大量病人感染、烧伤等伤害、死亡案件。将人工智能应用在制造、交通、医疗、教育等重要领域的过程中会发生侵害人身、财产安全的事故和危险，成为不可忽视的安全风险，无疑构成法律上的侵权。

之所以会出现人工智能应用的侵权问题，一是由于人工智能本身具有的复杂性和不可预见性；二是技术和应用处于萌芽阶段，产业发展只关注创新、市场和经济效益，安全因素未能充分考量④；三是有关人工智能应用的法律法规、行业规范、责任体系等较应用水平来讲相对滞后和缺失，安全监测和行业监管不明确，应用处于混乱和原始的状态，因此应用过程中的人身安全威胁成为首当其冲应当考虑的安全问题。

然而人工智能应用的自主性、独立性、拟人性使侵害责任划分面临责任主体、归责原则等的复杂性。以自动驾驶汽车致人死亡案件为例，交通法中侵权责任的划分首先是按照过错责任原则追究驾驶员的责任，但是当汽车处于自动驾驶模式时驾驶员对汽车是没有操作的，驾驶员此时对汽车安全行使的注意义务就转移到自动驾驶系统上，按照侵权责任法的归责原则是以行为人的行为为基础追究责任的，这种情况下就无法追究驾驶员的过错责任。正如美国优步汽车撞死行人的案件中，司机没有驾驶不承担侵权责任，而自动驾驶系统也不是责任主体，因而对行人的侵权责任无人承担，这对被侵权者来说显然是不公平的⑤。该案例引起各方对无人驾驶汽车安全性的顾虑，如何衡量其安全性，如何设立无人驾驶汽车的通用安全标准，如何处理司机与无人驾驶的角色分工，如何划分各方侵权责任等等一系列问题都亟需法律给予规范。

2.数据信息安全与隐私权风险

关于隐私、个人数据保护等问题的讨论自互联网快速发展以来就是学者研究的重点和难点，但不同于之前的是，风险的防控目的已经由防止不合理的攫取信息谋取不正当利益转为协调数据作为人工智能发展的基础和保护个人隐私的权益之间的取舍，这是由人工智能发展的云计算、大数据技术是人工智能发展的基础，数据的收集和挖掘是智能水平发展的重要动力来源。人工智能发展规划提出既要为人工智能发展建立海量数据的大数据资源，但又要强化数据安全和隐私保护，为数据风险和智能发展提出较为中立的态度⑥。美国科技网站 Techcrunch 专栏作家 Natasha Lomas 评论称，人工智能对数据的需求量是巨大的，比互联网、大数据等的需求都要大，因为机器学习依赖于海量数据的驱动才能发挥功能提高智能水平[14]。如智能聊天工具就是通过对用户手机中的信息、通讯、聊天习惯、购物等许多信息的获取的分析，才能在和人类交谈的过程中更加了解人类，达到图灵测试的效果，而这样就使个人在人工智能应用面前变为“透明人”。

人工智能应用的深度学习技术是在数据基础上发展的，数据是人工智能应用的前提和基础。人工智能时代下个人信息和数据的威胁主要来自两点，一是智能系统漏洞和黑客攻击本身带来的数据泄露的潜在风险，二是由于目前个人一味追求互联网、人工智能带来的便利而对个人信息的保护意识低下，人工智能企业为了追求利益而对个人信息以明示或默示的形式加以收集、利用、倒卖，从而使个人在精准营销的便利中落入精准诈骗的圈套，最终

给个人人身、财产等都带来了巨大隐患。

人工智能在指纹识别、面部识别、语音识别以及通过各种应用对个人隐私进行学习的过程中，精细地记录着个人生活，掌握个人隐私，让侵犯个人隐私的行为更加方便，需要相应的法律和标准对个人隐私给予更有力的保护。当前对隐私的保护模式采取的是“同意收集”的模式，即对隐私信息的管制包括对使用者明示或未明示同意的收集。利用人工智能技术很容易推导出公民不愿意泄露的隐私，例如从公共数据中推导出私人信息，从个人信息中推导出和个人有关的其他人员（如朋友、亲人、同事）信息（在线行为、人际关系等）。这类信息超出了最初个人同意披露的个人信息范围。

三、人工智能应用安全风险的法律防控

法学对风险社会问题的研究的重点是法律制度与法律秩序，在安全风险的管理中，哪怕是一个细枝末节的危险因子或者可能性较小的灾难势头，都应当由法律规则和法律秩序来规范和预防[15]20。因此，法律明确人工智能应用范围和程度是预防和解决安全问题的重要防控途径。

（一）法律原则：人工智能法律人格定位

人工智能“拟人性”的行为特征，使人们怀疑可以自主决定的人工智能应用是否会取代人类，挑战人类主体地位。同时人工智能在应用过程中的类人性也对现行法律关系造成挑战，法学领域对其法律人格进行了讨论，目的是为了在人工智能参与下的社会关系，明确人和机器的权利、义务关系和责任体系。人工智能是否可以获得法律人格或者说是法律主体资格，意味着人工智能是否可以成为法律上的“人”。当前法学领域关于人工智能法律人格的讨论呈现出否定说和肯定说两种相反的观点：

第一种是对人工智能法律人格持否定态度，主要有王利明、吴汉东教授的客体控制说和郑戈的工具说。吴汉东教授认为从法理学主客体二分法来说，人工智能不是有生命的自然人也非有独立意志的法人，是受法律主体控制的机器人，不足以取得独立的主体地位[15]5；王利明教授从人工智能产生的属性即代替人类从事一定行为，是作为客体而出现的，不能独立享有权利和承担义务，现行的法律体制和规则可以解决人工智能带来的挑战，没必要赋予其民事主体资格[16]；郑戈认为人工智能作为人类的工具，造成伤害以后承担责任的还是人，赋予其法律主体地位是多余的[17]。

第二种是对人工智能法律人格持支持态度，主要有电子人说、有限人格说和电子代理人。将人工智能视为电子人在实践中初见端倪，欧盟、韩国、爱沙尼亚对人工智能“电子人”或“代理人”已经表现出了立法动向[18]。郭少飞则从实践、法史以及自主能力的本质属性认为人工智能符合“电子人”的要求⑦。袁曾认为人工智能作为有独立意识的智慧工具，应当享有权利承担义务具备法律人格，但是与自然人和法人人格不同的是，人工智能承担责任的能力有限，因此应该采用有限人格。电子代理人实则是将人工智能看作了人的“代理人”，因为代理人本质上也是具有法律人格的人。有学者以“自主意识”为标准，认为人工智能发展过程中，人工智能会由原来的保守“工具论”最终实现“拟制论”的转变[19]。

以上各位学者支持或否定的态度是从人工智能是否具有“自主意识”以及法律主客体要素等进行分析，可谓“百花齐放，百家争鸣”。但从人工智能本质及安全角度来看，笔者赞同第一种观点，认为人工智能应用法律人格的态度应当更加保守和谨慎，科技和时代的发展推动着法律的变革，但并非新兴事物的产生都必然引起传统法律价值和法律框架体系的变化，尤其是与人类越来越相似的人工智能，更应当采取理性的态度去对待。美国著名哲学家希拉里·普特南认为，人工智能法律地位的有无不是科技发展程度决定的，而是法律是否赋予它主体资格[20]。从人工智能本质属性出发，任何科技进步和发明都是由人类为主导创造并服务人类的工具，自产生之日便不具有和人平等的法律属性。人工智能只是帮助人类的工具，不具有自然人的独立意志，不能赋予其法律主体地位[21]。之所以会产生法律人格的观点无非是工具能够像人类一样有智慧，但仍不能改变它作为工具的属性。基于以上分析以

及安全为核心的法律价值，笔者对人工智能应用法律人格采取否定的态度，即仍将人工智能应用视为人类智能延伸的工具，坚持人工智能“工具论”的法律客体原则。

（二）法律规制：人工智能应用的负面清单

对于人工智能的应用，应当按照其对于安全的影响划分为自由应用领域、限制应用领域和禁止应用领域，采用负面清单制度明确限制应用领域和禁止应用领域，并分别采用许可制及严格禁止的方式予以规范。

1.自由应用领域的自由生产制度

人工智能应用整体是符合社会发展要求的，技术的越来越成熟在很多领域的应用是符合安全和发展双重要求的，因此在产业升级背景和社会化应用中可以自由应用，除法律明确限制应用和禁止应用的领域之外，均应以自由生产为原则，允许企业自由应用人工智能技术并自由生产。

2.限制应用领域的审批制度

自主意识是人和机器最大的差别，人工智能目前虽然已经可以具有独立意识，可以做出独立的行为，但仍不具备人类的情绪和感情。但是人工心理和人工情感的研究在世界范围内都处于热门研究领域，世界上研究带有情感的机器人最先进的国家就是日本[22]。在应用领域儿童和老人陪伴机器人可以赋予一定情感，这不会危及人的安全，也不会引起法律、伦理方面的挑战。然而像电影《人工智能》中出现的人工智能孩子、人工智能性伴侣等都是像人一样拥有感情和情绪，他们的应用不仅引起了伦理风险，还会在收养、婚姻制度等方面引发风险。当然电影中的都是科幻色彩，但是随着技术的进步，使机器富有情感不是没有可能，但在应用范围中应当予以严格的限制。

有学者认为人工智能情感和自主意识应当为技术禁区，因为自主意识作为机器和人最大的区别，禁止人工智能拥有自主意识是保证人作为这个世界唯一能够意识到“我”的独立存在的个体，是保证人自身安全的最重要的屏障。王治东教授认为人工智能如果有了“我”的概念和意识，不仅是对人的模拟，而且具有了人的核心内核。在这个层面而言，人工智能就在个体上可以成为另一个物种的“人”[23]。而人工智能一旦有了“我”的自我意识，就会视人类为异类，这时将会对人类生存造成实质的威胁。但具备情感和自主意识的人工智能技术应用于孤独人陪伴、自闭儿童治疗等方面却有着不可替代的作用，基于此，笔者认为在坚持人工智能“工具论”的法律原则之下，对于人工智能情感和自主意识技术应用的领域，应确定为限制应用领域，并通过审批制度予以法律监管。

同时，限制应用的领域要使人工智能的自主化程度和智能水平处于人类可控制的范围。人工智能应用作为人类的工具必然有超过人的强大的能力，但随着其深度学习能力加深，智能是否会超过人类智能仍是未知，因此要确保人类对其应用程度的把控。如哪些事情可以由智能系统自行决定，哪些又必须靠人来决策，对于限制应用的领域，只有符合安全标准并得到安全许可才能投入商业应用[24]。

3.禁止应用领域的严格禁止

正如克隆技术在成功克隆出一只羊，又克隆出一只狗、一只猪，尽管技术已经成熟，但是无论如何都不能允许克隆人，克隆人不仅面临复杂的道德伦理困境，还会面临人的生存问题的挑战，因此，目前全世界法律均禁止克隆人。但是这一技术不是绝对的被禁止，应用在克隆器官方面在医疗领域却是一大进步，对人类健康和生命也是有利的。相比较而言，人工智能更具有复杂性和不可预测性，对于全人类造成危险并颠覆人类的人工智能技术，应确定为禁止应用领域并严格禁止。首先被确定为禁止应用的应是智能自主武器的应用，其他可能会被毁灭甚至颠覆人类的人脑技术也应限制于研究领域，明确禁止这一技术的生产应用。

随着人工智能技术的发展，其应用的安全风险是不可避免。法律对于技术调控的核心在于规范技术的应用，在鼓励技术发展、转化之余，更应当站在安全的视角，对技术应用加以安全风险防范，使技术应用达到最大限度的安全，真正促进人类社会的发展。人工智能时代追求高速、自由发展应当充分考虑到安全这一人类的基本需求，并立足当下分析存在的安全风险，明确人工智能与人的关系，建

立多层次的人工智能发展规范和模式，走向实现健康、安全、稳定的人工智能新时代。

注释

①中国电子技术标准化研究院.人工智能标准化白皮书.2018.1.

②华春雷.人工脑连接体：类脑人工智能的奇点时刻来临.华春雷科学网博客.

③向家莹.五大银行集体裁员撤点　竞速“智能化转型”.经济参考报.2018.4.9。银行柜员的工作和部分银行网点已经被裁撤掉，主要的几大银行如工行、农行、建行等纷纷裁员，预计每家银行接近有上万人失业，取而代之的是智能化网点和柜台、以及智能客服。中国银行的年报提出了智能化网点超过百分之八十覆盖率的目标。

④央广网.高交会官方回应机器人伤人事件：员工操作不当所致.2016.11.19，世界机器人大会秘书长、中国电子学会副理事长徐晓兰表示，我国服务机器人的应用还属于萌芽状态或是试用阶段，但很多企业忙于或是急于做市场推广，更多的是注重它的功能和应用，而对安全方面的设计恰恰是它的弱点。这次事件给我们带来了一个警示，提醒我们要更加注重服务机器人的安全设计。

⑤曹建峰.全球首例自动驾驶致死案背后，“谁来担责”的法理探讨.腾讯研究院.

⑥2017年7月国务院《新一代人工智能发展规划》.中华人名共和国政府网.

⑦郭少飞.“电子人”法律主体论[J].东方法学.2018：10.他认为人工智能可以作为电子人的依据在于：实践中人工智能主体已有成例或官方建议；历史上，自然人、动物或无生命体法律主体的演化表明，存在充足的法律主体制度空间容纳　“电子人”；法理上，现有法律主体根植之本体、能力与道德要素，“电子人”皆备。由外部视之，人工智能现有及潜在的经济、社会、文化、伦理影响以及对哲学范式的冲击，促使既有观念、模式、体系开始转换，“电子人”的法外基础已然或正在生成并强化。

参考文献

[1]格雷亨姆.人工智能入门[M].北京：机械工业出版社，1988：1.

[2]马少平，朱小燕.人工智能[M].北京：清华大学出版社,2004：2.

[3]翟振明，彭晓芸.“强人工智能”将如何改变世界——人工智能的技术飞跃与应用伦理前瞻[J].人民论坛·学术前沿，2016（7）：22-33.

[4]李建中.科技丰碑[M].北京：中国科技技术出版社,2009：493.

[5]祝叶华.“弱人工智能+”时代来了[J].科技导报，2016（7）：67-69.

[6]鄂大伟.中国人工智能未来十大发展应用方向[J].中国工业报，2018（3）：22.

[7]马斯洛.动机与人格[M].许金声，等，译.北京：华夏出版社，1987：44.

[8]博登海默.法理学：法律哲学与法律方法[M].邓正来，译.北京：中国政法大学出版社，2017：232-320.

[9]杨帆.人工智能技术应用的伦理问题研究[D].昆明：云南师范大学，2015.

[10]马尧.亚太军情观察——未来军用机器人会"造反吗？[EB/OL].（2018-03-21）http://sh.qihoo.com/pc/9d68ed16e483f3557?sign=360_e39369d1.

[11]霍金.人工智能的威胁就像核武器——世界将发生10大变化[J].花炮科技与市场，2017（4）：27-28.

[12]刘耀会.关于人工智能与社会伦理的探讨.机器人技术与应用[J].机器人技术与应用，2017（5）：44-48.

[13]鲍达民.中国近半岗位或被人工智能取代[J].中国邮政，2017（5）：7.

[14]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，216（21）：19.

[15]吴汉东.人工智能时代的制度安排与法律规制[J].法律科学（西北政法大学学报），2017（5）：128-136.

[16]王利明.人工智能时代对民法学的新挑战[J].东方法学，2018（3）：4-9.

[17]郑戈.人工智能与法律的未来[J].探索与争鸣，2017（10）：78-84.

[18]姚万勤.人工智能影响现行法律制度前瞻[J].人民法院报，2017（2）：54.

[19]孙占利.智能机器人法律人格问题论析[J].东方法学，2018（3）：10-17.

[20]张玉洁. 论人工智能时代的机器人权利及其风险规制[J]. 东方法学，2017（6）：56-66.
[21]田小军，徐思彦，何帆. 文化产业+人工智能的发展与前沿法律政策[J]. 中国出版传媒商报，2017：20.
[22]王志良. 人工心理与人工情感[J]. 智能系统学报，2006（1）：38-43.
[23]王治东. 人工智能风险性刍议[J]. 哲学分析，2017（5）：31-39.
[24]杜严勇. 人工智能安全问题及其解决进路[J]. 哲学动态，2016（9）：99-104.

Security Risks and Lawful Prevention and Control of AI Application

Zhang Min Li Qian

Abstract: Known as the starting point of Artificial intelligence, the year 2017 has witnessed a step-by-step breakthrough and application across various fields of artificial intelligence accompanied with a series of security risks. This article made an analysis of security risks at three levels including the threat of AI application to human security, social ethics security and personal security covering person's life ,data, privacy and consequently reached a conclusion that AI application should be given a lawful regulation ranking from free application to limited application to ban on the basis of lawful object of regarding AI as a tool.

Key words: AI Application; Security Risks; Lawful Prevention and Control; Legal Personality