人工智能商业应用中的安全问题

林 Hongzhen *
武汉科技大学恒大管理学院，中国武汉，
996672199@qq.com，通讯作者

石漆彭
武汉科技大学恒大管理学院，武汉
1321248247@qq.com

Zhipan 余
武汉科技大学恒大管理学院，武汉
937672021@qq.com

Bo 扁
武汉科技大学恒大管理学院，武汉
543182731@qq.com

摘要

本研究旨在探讨人工智能技术在商业应用中的安全问题。运用文献研究法，正确认识和分析人工智能带来的商业安全问题。这些问题主要包括个人安全问题、数据安全问题和隐私安全问题。造成这些问题的主要原因有:相关法律制度不健全;人工智能安全技术不够成熟;以及人工智能安全标准标准化不足。本研究得出的有效解决方案主要包括:加快人工智能立法;加强人工智能安全技术;完善人工智能安全评估管理。

CCS 的概念

• **计算方法;**●人工**智能;**

关键字

人工智能，安全，设计

ACM 参考格式:

林宏振*，于志攀，彭世奇，边波。2021.人工智能商业应用中的安全问题。第*三届人工智能与先进制造国际会议(AIAM2021)， 2021 年10 月 23 日至 25 日，英国曼彻斯特*。ACM，纽约，美国，4 页。https://doi.org/10.1145/3495018.3495359

1 介绍

近年来，随着科技的进步，人工智能技术在语音识别、军事应用等诸多方面都取得了巨大的进步。但到目前为止，我们在人工智能方面面临着两个最大的问题。其一，技术发展并非如此

AIAM2021, 2021 年 10 月 23 日至 25 日，英国曼彻斯特
& # 169;2021 计算机协会。Acm isbn 978-1-4503-8504-6/21/10…$15.00
https://doi.org/10.1145/3495018.3495359

够了，二是在应用过程中会出现很多实际问题。然而，人工智能的应用越来越广泛，由此带来的安全风险也成为我们不得不关注的问题[1]。然而，在我们的现实生活中，应用场景是非常开放和宽松的，传统的人工智能是基于大数据和经验规则，这使得人工智能很容易受到外界的影响[2]。本选题主要针对人工智能发展的初级价格区间，从人工智能在商业应用中的安全性角度进行分析。一方面，我希望设计师以实用性为目标，同时不要忽视人工智能的安全问题。另一方面，只有对人工智能的不足有了更深入的认识，我们才能更加客观、冷静地对待智能机器，为人工智能的长远发展奠定思想基础，对现阶段的问题给出相应的思考。

2 文献综述

2.1 国外研究综述

1956 年以前，人们开始探索机器如何取代人力。在亚里士多德的三段论中，培根给出了基于归纳法的较为系统的研究思路，这些都对后来的人工智能研究产生了重大影响。1956 年夏天，麦卡锡使用了“人工智能”这个术语。第一次在学术研讨会上[3]。费根鲍姆所研究的专家系统的分析能力甚至超过了同时期西方国家的化学研究人员。然而，20 世纪 70 年代以后，人类在计算机的发展方面相对落后，这使得人工智能的研究实际上毫无用处。科学家称这一时期为“人工智能之冬”。1997 年，计算机系统“深蓝”与世界围棋锦标赛成功对弈，这也标志着人工智能真正可以完成大量属于人类思维的任务[4]。

2.2 国内研究综述

上世纪五六十年代，人工智能刚刚诞生，但新中国刚刚成立的时候，中国还没有人在做研究。直到 1978 年 3 月，国家科学会议都是

举行。此后，钱学森等人主张研究人工智能。遗憾的是，由于当时的研究刚刚起步，很多人将人工智能与特殊功能混为一谈，发展缓慢。改革开放后，为了发展人工智能，我国派遣了许多青年学者到国外学习先进的人工智能理论知识。然而，“人工智能”当时并没有直接提到。进入 21 世纪后，更多关于人工智能和智能系统的研究课题获得了国家自然科学基金的重点和重大项目。中国人工智能领域的研究也被提升到国家战略的高度。机遇和挑战也做好了充分准备[5]。

3 人工智能在商业应用中的主要问题

3.1 人身安全问题

1978 年，世界上第一个机器人“杀人”。发生在日本广岛。当一名工厂工人值班时，机器人发生故障，将其切割成钢板。不幸的是，这发生了。1985 年，在一场人机国际象棋比赛中，赢得前苏联国际象棋冠军的古德科夫被机器人棋手释放的高压电流触电。机器人因为三连胜而生气。那里的程序出现了异常，导致了悲剧的发生。

2018 年，世界上第一辆无人驾驶汽车在美国亚利桑那州造成一人死亡。一辆优步无人驾驶汽车在行驶过程中发生故障，无法准确识别人行横道外的行人，导致一名女子当场死亡。在战争中使用人工智能武器造成的意外伤害也很常见。例如，无人机在打击目标时，如果使用分散弹头和多弹头，就无法准确锁定目标进行精确打击，或者锁定目标是假装伪装的，人工智能武器无法准确识别。这些识别错误会造成大范围的意外伤害。2004 年至 2012 年间，美国使用人工智能武器对阿富汗境内的恐怖组织进行了约 400 次空袭。人工智能武器造成的儿童和平民死亡人数已达数万人。人工智能装备在战争中的应用，使国家人道主义化。学说已经跌入了无尽的深渊[6]。

3.2 数据保安问题

人工智能是互联网、大数据、机器智能叠加呈现的新一代风向标。当政府、企业和社会组织在维持各自的运作时，越来越多地依赖于大规模的数据收集、分析和使用时，整个社会的运作也在以数字化、透明化的形式顺利进行。人工智能时代的到来，要么将个人隐私暴露在阳光下，要么沉溺于黑暗之中，而且

让人身上的小雕像变得透明，也为“隐私保护”的必要性打上了大大的感叹号[7]。在日常生活中，人们为人工智能产品服务已不再少见。如地图导航、人脸识别、语言辅助功能等，都体现了人工智能与人类的密切关系。大型智能机器每天 24 小时在互联网上收集和整理你的个人数据信息，包括你的姓名、年龄、电话号码、地址、位置等。通过简单的分析和归纳，可以描绘出用户的个人习惯、饮食习惯和购物偏好。并且，通过进一步描绘个人信息，如个人的动作轨迹、交流范围、性取向等，可以生成用户画像。由于系统安全漏洞、黑客攻击等原因，一些非正式专业网站的个人数据存在泄露、被盗、交易等安全隐患[8]。

3.3 私隐及保安事宜

2018 年 3 月，据英美媒体报道，剑桥分析公司未经授权获取美国社交媒体脸书 5000 多万用户信息，设计软件分析用户政治意图，预测和影响选民投票。这一重磅事件的负面影响大大降低了 Facebook 的商业声誉，严重侵犯了公众的合法权益，引发了公众对隐私的反思。在人工智能快速发展的时代，企业未经许可滥用用户数据挖掘商业价值的现象并不鲜见。隐私保护面临前所未有的危机[9]。现代人类文明的发展越来越离不开数据，人工智能的产生和进步也与大数据密切相关。这些数据在被收集和汇总时，必然会涉及到人们日常生活、工作、人际关系的方方面面，对个人隐私泄露构成了极大的威胁。大多数用户在使用智能软件时出于信任会按要求提供相应的信息，但用户并不知道自己的信息可能被收集和使用。这是人工智能发展过程中，数据收集者或控制者未经用户授权泄露个人信息的行为。因此，人工智能时代的数据安全和隐私保护是非常关键的核心问题。正如艾瑞斯所说:“个人隐私在一定程度上不是数据分析的问题，而是数字化过程的阴暗面”[10]。

3.4 法律困境

随着人工智能技术的稳步发展和成熟，虽然极大地便利了人们的日常生活，促进了社会系统的正常运行，但它始终是个人隐私泄露和数据泄露威胁的隐患。一些法律制度带来了巨大的影响和挑战。

当机器人在某些任务上可以完全取代人类，当机器人被越来越多的人所认识，谁应该为机器人所犯的错误负责？是机器人的开发者还是

机器人本身? 机器人能承担责任吗? 如果他们做不到或做错了人的责任，谁来承担责任? [11]

2009 年 10 月，英国一名司机按照 GPS 导航规划的路线正常行驶，却不小心冲下悬崖，撞坏了别人庄园的栅栏。尽管英国法院最终将事故归咎于 GPS，但它仍然认为司机因粗心驾驶而负有责任。虽然这是一起由技术而非人为造成的交通事故，目前的法律法规与之不匹配，但法院往往会做出不利于人类的判决。显然，人工智能时代的到来，让原本直白的法律条文的适用性受到了质疑:人类的过错所造成的恶果，为什么要由人类来承担? 当代人工智能与传统的人工智能有很大的不同。它不再仅供人类使用，而是由人类部署[12]。一旦部署，人工智能机器将不再根据收集和分析数据的指令独立运行。从这个意义上说，以前不能起诉机器人的观念需要根据人工智能的发展来改变。

4 解决人工智能安全问题的措施

4.1 加强人工智能安全技术

加强信息加密技术。信息的加密程度与人工智能设备的安全性密切相关[13]。对于人工智能的数据处理和计算量，传统计算机系统的固态硬盘无法承受人工智能复杂性带来的巨大计算量，信息加密程度也会降低。传统计算机已经不能满足人工智能安全维护的需求。但如果将数据通过量子计算机进行处理和呈现，一方面可以获得量子加密，保证人工智能维护的安全性，另一方面可以提高数据传输的效率，提高数据系统的稳定性。确定合适的系统载体。系统载体是人工智能信息安全的基础和保障。但是，已知的各种系统都存在明显的操作系统漏洞，需要在后续的维护服务中进行升级和修改。因此，仅使用市场上的操作系统并不能保证 AI 设备的安全性，不存在风险。这从根本上决定了 AI 需要开发一种新的编程语言，建立独立的数据库来获取信息。除了预留信息接口和资源数据共享外，机器系统还需要能够通过其独特的传感器接收外部信息，如语音、触摸等，从而进行正常的数据处理和交互，保证人工智能信息的安全性。

提高人工智能的可控性。人工智能的目标是深度学习和自主控制，这就有可能给人类社会带来不确定性风险。为了…将这种风险降低到可接受的范围内，人工智能设备需要人的控制和干预。因此，人工智能的设计专家在研发过程中需要考虑人工智能意识形态的调节和控制;D、实现对人工智能设备的有效管理，确保人工智能在相应领域发挥优势而不被滥用。

4.2 建立人工智能安全标准规范

对人工智能设备的控制是保证人工智能安全的关键。为了保证人类对人工智能设备的控制，相关部门需要建立人工智能安全标准和规范。研究人员在进行人工智能研究前，应向有关部门报告，获得相应的认证和批准后，方可进行人工智能的研究和开发，以确保工作不违反社会基本规则，维护人工智能设备的安全。同时针对人工智能设备运行中的缺陷和错误提供解决措施，进一步为人工智能的安全保驾护航。

完善人工智能安全评估管理。完善人工智能安全评估管理是减少人工智能设备安全问题的有效途径。在研发过程中;D、人工智能研究者要不断完善和完善对人工智能的评估和管理。通过安全评估，人工智能研究人员应及时发现系统存在的不足和缺陷，避免人工智能在生产过程中出现安全问题。因此，空气&D 人员需要在日常设计研究和生产过程中采用动态管理方法，加强对人工智能设备的监管，不断调整评估管理，构建人工智能安全评估模型和仿真机制;通过 Statistics Measure 的知识，对人工智能在各个设计和生产环节可能出现的安全问题进行预估，并提前制定相应的解决方案，降低人工智能安全问题的风险。

设计人工智能的道德机制。研究者应高度警惕人工智能设计过程中的道德风险，制定相关的人工智能道德机制，赋予人工智能基本的道德评价和判断能力，确保人工智能在与人类互动过程中做出的评价和判断符合当前社会的道德标准。同时，在人工智能无法合理、准确判断对方和自身的行为是否符合基本道德标准的情况下，增加了人工智能的自动停止功能，以避免在与人类互动过程中，由于对方的错误判断或恶意控制、利用而导致的错误行为。通过增加人工智能道德机制的设计，既赋予了人工智能在可控范围内的最大自主权，又保证了人工智能的使用安全性。

4.3 完善人工智能相关法律

随着人工智能技术的不断创新和发展，也带来了一系列的法律问题。例如:人工智能造成的信息泄露和个人陪审责任的问题。目前，我国在人工智能方面的法律还存在很多空白。因此，有关部门应高度重视人工智能立法工作，及时安排宏观立法。法律人员可以从一些相对成熟的技术领域开始制定法律法规，逐步形成完整的人工智能法律体系，为人工智能未来发展中存在的法律问题打下坚实的基础。

5 结论

随着科学技术的不断进步，人工智能进入了一个快速发展的阶段。人工智能的深入研究和广泛应用，也引起了更多人对人工智能安全性的关注。虽然人工智能的使用和运行可能存在安全隐患，但我们绝不能把人工智能扼杀在摇篮里。相反，我们应该积极采取有效措施，从法律、技术、制度和伦理等方面避免人工智能的出现。各个生产和应用环节的安全问题，使得人工智能在其优势领域发挥重要作用，成为人类的好帮手。

致谢

本研究得到中国国家社会科学基金资助，项目名称: 基于风险控制的理工科大学创业法学教育研究(批准号 BIA170192)

参考文献

[1] 陈玉飞，沈超，王茜，等。人工智能系统的安全和隐私风险。计算机研究与发展，2019,56 (10): 111 - 126
[2] 袁立科。人工智能安全风险挑战与法律应对。中国科技论坛，2019,274 (02): 9 - 10
[3] 徐大海。人工智能系统的安全和隐私风险。电子技术与软件工程，2020,No. 176 (06): 236 - 237
[4] 魏伟，景慧云，牛金星。人工智能数据安全风险与治理。中国信息安全，2020，第 123(03)期: 83 - 86
[5] 他哲。走向人工智能时代。电子政务，2016(12):9
[6] 廖天翔。人工智能安全分析。中国科技投资，2018(5):291
[7] Ailun 表示。首选。人工智能安全与治理。信息安全与通信保密，2019(10):13-15
[8] Bi 中豪。人工智能安全问题及对策研究。中国新电信，2019(1):136
[9] 易凯凡，邵谦，陈敏。人工智能安全:逆袭分析。计算机科学与应用，2019,9 (12): 10
[10] 陈。尾戒缠住了基于人工智能的网络安全防御系统设计研究。中国新通信，2019,V.21 (15): 154 - 155
[11] Wan HAOGE。人工智能技术与互联网安全的结合探讨。科学与信息2019，(02): 52-52
[12] 王兴伟，李丹，苏金树，等。2019 年智能网络理论及关键技术介绍。计算机研究与发展，2019,56(5): 907 - 908
[13] 刘东海，方超，冷正华。人工智能在安全管理中的应用。建筑安全，2020 (9): 31-34