人工智能窃取人脑灵感算犯罪吗

手机和电脑就是一工具。人工智能就一软件...^_^

人工智能和机器学习如何影响网络犯罪分子使用的恶意软件类型

通过大数据分析以及公安系统身份证识别匹配,以及人脸识别语音声纹比对。未来采集血液DNA.所有大数据汇集到云端实现人工智能?

法律盲区:人工智能犯罪谁负责

试想,2023年自动驾驶车穿梭于大街小巷。若不幸发生了交通事故,行人被撞身亡,媒体将争相报道。这场官司必将引发广泛关注,但究竟该如何审判,依据是什么?

如今,英国布莱顿大学的JohnKingston给出了一个答案,但有些差强人意,他提出了AI领域的刑事责任理论,并指出自动化、计算机和法律领域需改变态度,谨慎应对等关键问题。

争论的核心在于人工智能系统能否自行承担刑事责任。Kingston称,以色列奥浓科学院的GabrielHallevy对此问题进行了深入研究。

构成刑事责任通常需要明确其行为和意图(法律术语为actusrea和mensrea)。Kingston称Hallevy描绘了AI系统可能涉及的三种刑事犯罪情况。

第一种情况为间接犯罪,肇事者为存在精神缺陷的人或动物,此类肇事者无需承担法律责任。但任何操纵精神病患者或动物实施犯罪的人均需承担相应刑事责任。例如,狗主人命令狗袭击他人。

再比如,智能机器的设计者及使用者。Kingston表示: "AI项目可能被当作无辜的工具,而利用它实施犯罪的软件编程师或用户则为间接犯罪的主谋。"

第二种情况为不可抗力与意外事件,即指因不当使用AI系统导致的犯罪。Kingston以日本摩托车工厂智能机器人杀人案件为例,解释道:"机器人将工人误认为危险对象,采取消除威胁的最有效方式,挥动力大无穷的液压悬臂,将毫无防备的工人推入机器,迅速结束了他的生命,然后继续执行工作任务。"

此案例的关键问题在于该机器的编程师是否已知此类机器的功能缺陷及可能带来的后果。

第三种情况为行为与意图兼具的直接犯罪,如果AI系统的作为或疏忽不作为构成犯罪,则可直接证明其犯罪事实。

Kingston认为,犯罪意图虽然难以界定,但仍具参考价值,他表示: "超速属严格责任犯罪。因此根据Hallevy的说法,自动驾驶汽车如果超速行驶,法律上有充分理由追究驱动该汽车AI技术团队的刑事责任。"如此看来,车主无需担责。

接下来,涉及刑事辩护。被追究刑事责任的AI系统将如何辩护?Kingston列举了几种可能:AI程序是否可效仿精神病患者,以系统故障为由进行辩护?或效仿人类被迫或醉酒犯罪,将受电脑病毒袭击作为辩护理由?

这几种辩护情况并非凭空设想,Kingston分享了英国的一些案例,有计算机犯罪的相关责任人就以机器感染恶意软件为由,进行过成功辩护,并称恶意软件该负责。

某案例中,一名被控发起拒绝服务攻击的青少年黑客辩称,木马程序发动了此次攻击,该程序还在警方介入前清除了作案痕迹。

最后,涉及刑罚类型。既然AI系统是犯罪行为的直接责任方,那么应由谁来接受何种刑罚?这些问题尚不得而知。

但若AI系统触犯的是民法,就不应再追究其刑事责任。接着问题来了,AI系统究竟属于服务还是产品?

如果将AI系统视作产品,应根据产品保修证所提供的信息,运用产品设计法规处理案例。

如果将其视作服务,则存在过失侵权。这种情况下,原告通常需提供构成过失侵权的三要素。其一,需证明被告有看管义务。Kingston表示,尽管AI案件中没有明确界定看管标准,通常可直接证明。

其二,需证明被告存在失职。最后,还需证明该失职对原告造成了伤害。

然而,比这些条文更复杂的是,随着AI系统的能力愈发接近人类,甚至超越人类, 其法律地位也将改变。

有一件事是肯定的:未来几年内,律师(或是替代他们的AI系统)会卷入越来越多的新奇案例纠纷中。

人工智能技术在安全方面将会面临哪些挑战

人工智能技术在安全方面将会面临以下挑战:

- 1.数据隐私和安全问题:人工智能系统通常需要大量的数据来进行训练和优化,这些数据可能包含用户的个人信息、敏感数据等。如果这些数据没有得到充分的保护和管理,就可能会引发用户的隐私泄露和安全问题。
- 2.技术瓶颈:虽然人工智能技术在许多领域取得了显著的成果,但仍然存在许多技术瓶颈,如过拟合、泛化能力差、模型不稳定等问题。这些问题可能会导致人工智能系统在实际应用中的效果不佳,甚至产生安全隐患。
- 3.算法局限性:目前的人工智能算法主要依赖于监督学习和深度学习,这些算法在处理复杂问题和模糊边界问题方面存在一定的局限性。这可能会导致人工智能系统在应对一些实际安全问题时,无法准确识别和处理潜在的威胁。
- 4.恶意使用和伦理问题:人工智能技术可能被用于开发新型网络武器、大规模假情报攻击和先进生物武器等,给国家安全和社会稳定带来严重挑战。此外,人工智能技术在伦理方面也存在争议,如自动驾驶汽车在紧急情况下的道德抉择等。
- 5.法律和监管问题:随着人工智能技术的发展,法律法规和监管措施跟不上技术发展的步伐,可能导致人工智能技术在安全领域的应用存在一定的法律空白。这可能会使一些不法分子利用人工智能技术进行犯罪活动,给社会带来安全隐患。
- 6.人才培养和意识问题:人工智能技术在安全领域的发展需要大量具备专业知识和技能的人才。然而,目前相关领域的人才培养和意识普及仍然不足,可能会影响人工智能技术在安全方面的应用和发展。
- 总之,人工智能技术在安全方面将面临诸多挑战。为了解决这些问题,有必要加强技术创新、完善法律法规、提高人才培养和意识普及等方面的工作。

人工智能犯罪如何看待

人工智能犯罪仅能归责于作为保证人的"自然人-法人"责任论。人工智能犯罪中"人心人性"的刑法常识观,应当确认人工智能犯罪的可归责主体,只能是作为算法安全社会关系主体的"自然人-法人"二元主体。

为妥当解决人工智能犯罪的归责原理和实践问题,应当在坚守人工智能犯罪"自然人-法人"二元主体模式的基础上修改完善刑法立法。