

title: 人工智能发展的现状与反思 speaker: 陈扬,林家馨,单宇航,杨一凡 plugins: - echarts prismTheme: solarizedlight

人工智能发展的现状与反思 { .text-landing.text-shadow }

By 陈扬,林家馨,单宇航,杨一凡 { .text-intro }

[:fa-github: Github](#) { .button.ghost }

1. 抛砖引玉--ZAO

最近一款名为ZAO的换脸app开始在各大社交网络刷屏。



操作简单、换脸逼真、还能圆一把明星梦.....

网友们纷纷感叹，ZAO好玩！AI厉害！

<slide class="bg-black-blue aligncenter" image="<https://source.unsplash.com/C1HhAQrbykQ/>" .dark" .size-130.aligncenter>

背后一些技术--deepfake

什么是deepfake?

2017 年，一名 ID 为 Deepfakes 的网友在 Reddit 网站上传了一段换脸视频，并在之后上传了一系列类似的视频；由于换脸视频涉及色情内容，并且侵犯了他人的隐私，引起了恶劣的反响。最终，Reddit 官方将 Deepfakes 封号。而作为报复，Deepfakes 也将换脸视频的 AI 代码免费公开。

!



一些观点

连色情网站都不敢瞎掺和的领域，ZAO居然来了，从技术和风险角度来说，ZAO的前景非常非常非常危险，已经不是在河边走了，这是在悬崖边翻跟头！

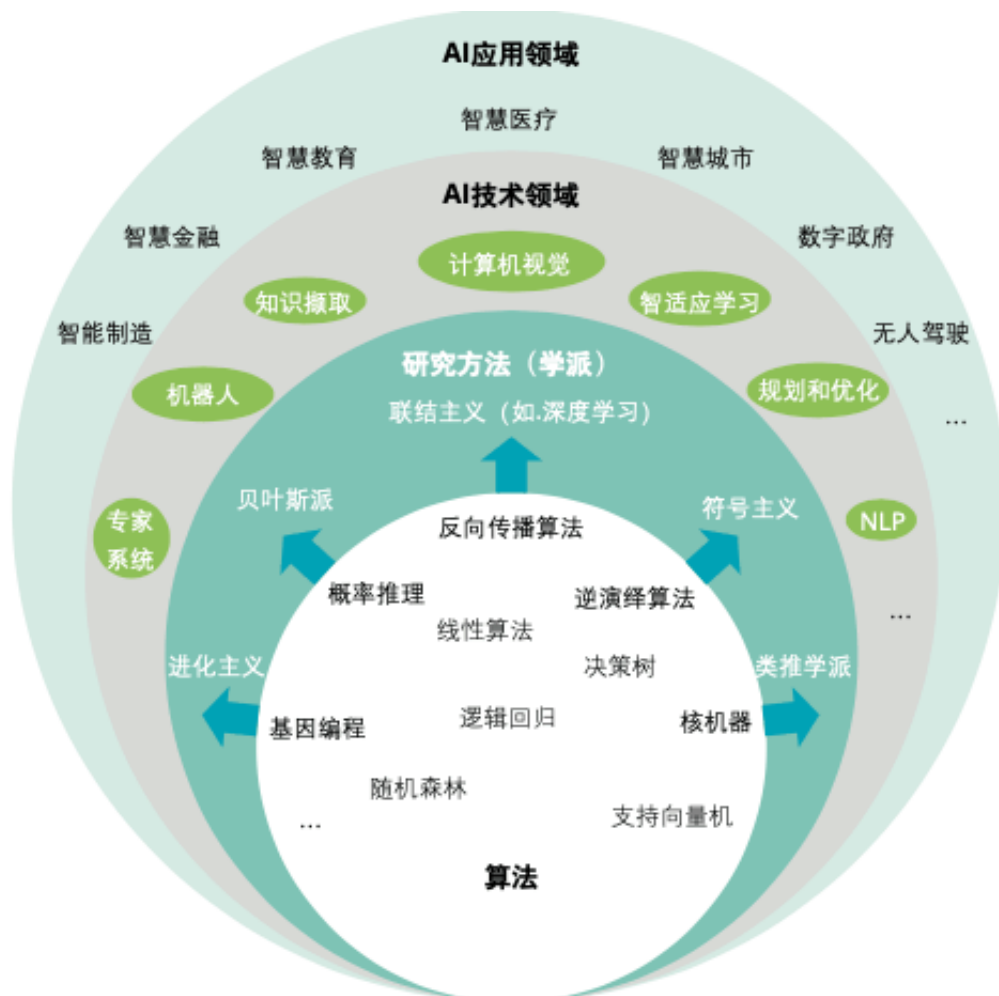
作为法律工作者，我认为ai换脸中有很多法律问题是有争议的:1、“ZAO”app涉嫌过度攫取用户授权，让你在无形中将你的肖像权拱手让人，以后你的脸将完全有可能被别人随意使用，变换；2、zao并未获得换脸明星们的肖像权授权，你变脸涉嫌侵权，但当明星认为自己的权利受到侵害时，“ZAO”app将完全有可能将法律的锅全部甩给你，让你自己承担侵权苦果。

什么是人工智能？

人工智能于一般教材中的定义领域是“智慧主体（intelligent agent）的研究与设计”[3]，智慧主体指一个可以观察周遭环境并作出行动以达致目标的系统[4]。约翰·麦卡锡于1955年的定义是[5]「制造智能机器的科学与工程」[6]。安德里亚斯·卡普兰（Andreas Kaplan）和迈克尔·海恩莱因（Michael Haenlein）将人工智能定义为“系统正确解释外部数据，从这些数据中学习，并利用这些知识通过灵活适应实现特定目标和任务的能力”。[7]

人工智能的研究是高度技术性和专业的，各分支领域都是深入且各不相通的，因而涉及范围极广[8]。人工智能的研究可以分为几个技术问题。

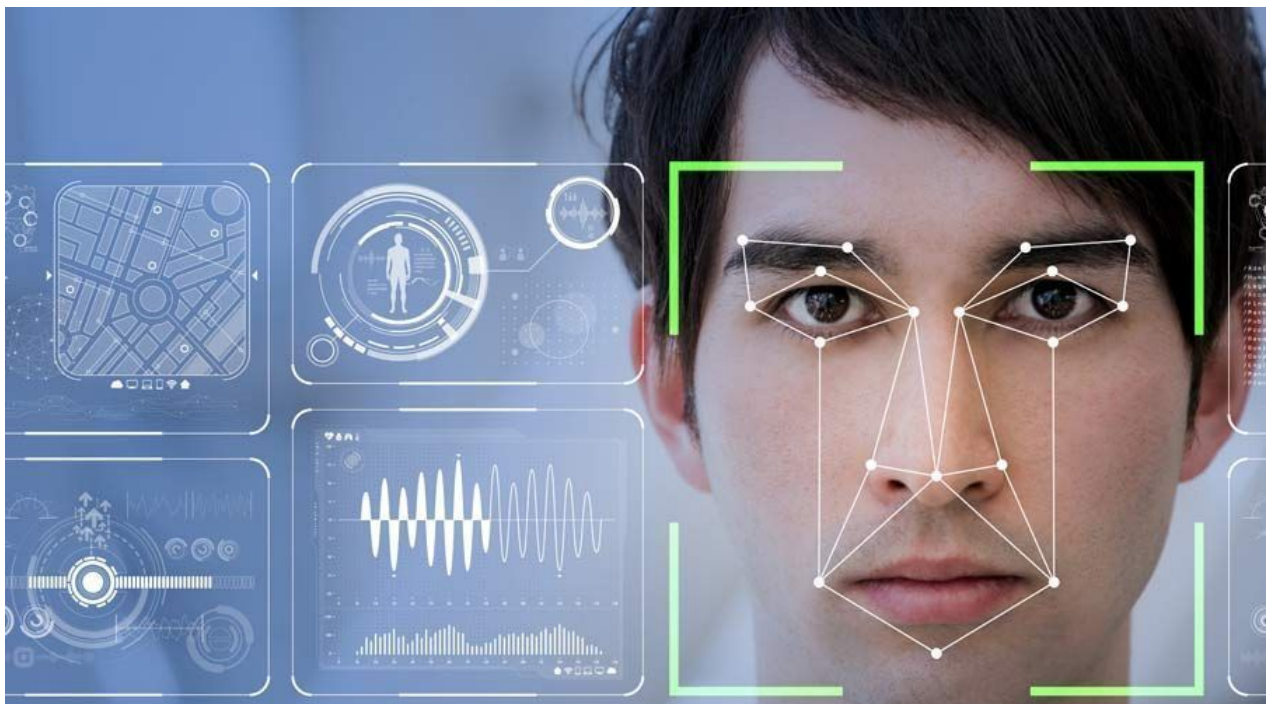
2. 人工智能广泛的应用



自然语言处理和计算机视觉



人脸识别



比如刷脸支付,微表情识别,疲劳检测等等应用

智能音箱 (Speakers)



“呐~有了这个音箱，每天都有人叫你起床，省了个女朋友了”。

自动驾驶



滴滴在国内也是率先投入带 AI 中

3. 人工智能的利与弊

在生活中其实广泛的运用着各种人工智能的计算,很多时候我们看似简单的应用,其实背后都蕴含着智能的一面

利:

人工智能可以显著提高人类的工作效率。比如,审核图片和视频,现在则完全可以交给机器,能快速过滤掉大部分无用信息,节省人力和时间。国内不少电商平台和快递公司配备了智能机器人进行快递分拣。这些智能机器人能识别出快递的面单信息,然后设计出最优分拣路线。

人工智能可以拓展人类的感知。人的感官只有耳朵、眼睛、鼻子、嘴巴等,人工智能可以拓展人类的感知能力和行动能力。少数人天生就有听觉障碍、视觉障碍等,人工智能可以弥补这些缺陷。

人工智能还可以帮助人类探索新的未知领域。有了先进的算法之后,结合数据做快速分析和跨领域综合比较,有望探索人类认知和心灵层面的东西。



弊:

第一个问题就是对就业的影响。首席执行官公开称颂人工智能将带来大量收益,但人工智能带来的主要收益就是降低成本。一家欧洲银行要求印孚瑟斯公司 (Infosys) 找到一种方法,将运营部门的职工人数从50000削减至500。这篇特别报道表明人工智能增强工具有助于减少像客服部门和人力资源部门的员工人数。麦肯锡全球研究院估计:到2030年,3.75亿人,即全球劳动力人数的14%,其工作岗位将被自动化技术所替代。企业家将决定是否职工提供就业再培训并支付相关费用,或者是否为职工提供再就业培训时间。很多企业表示愿意培训职工,让其掌握新技能,但企业不去承担费用。

第二个问题就是在人工智能普及阶段，如何保护个人隐私。利用互联网，已经可以对人们操控数码设备的行为进行详细记录。人工智能能为企业提供更好的工具，在线上 and 线下对顾客和雇员进行监控。如果企业通过此行为为顾客提供个性化服务或定制促销活动，顾客有时会高兴地接受。但人工智能肯定会侵犯隐私，这让人难以接受。例如，人脸识别技术已经变得十分先进了，甚至可以用来检测一个人的性取向。如果此技术被别有用心的人利用，将不利于公平公正。在有滥用监控技术和侵犯人权的国家，已经利用人工智能来监视政治活动和压制异见。世界各国的执法官员将利用人工智能技术发现罪犯，但也可利用其来窥探普通公民。需要制定新法律来界定监控的合理级别。

第三个问题是人工智能对商业竞争的影响。现在，很多软件公司竞相为企业提供更强大的人工智能增强工具。在人工智能领域取得突破的科技公司将行业竞争上甩开对手，甚至让对手出局，降低了市场竞争。以零售业为例，说明大公司如何利用人工智能获取市场份额。亚马孙公司通过大规模采用人工智能，掌控了美国电子商务的40%份额，其还利用人工智能构建壁垒，让竞争对手更难与其竞争。人工智能也将加剧某些行业的竞争。

4. 解决措施

现阶段是人工智能发展阶段（一个重点，两个方面）

重点从发展的技术层面进行规制，严格把控技术关口，防止技术运用的无序泛滥

一个方面是解决人工智能设计的包括知识产权、人格权、肖像权、隐私权等常规法律问题；

另一个方面是国家立法的同时加强行业内部标准制度的统一建立，达成某种技术开发商的共识，由技术人员内部进行纠正抵制

长远来看：

人类必须对人工智能绝对控制，并受到预先设计的有限教学程序的限制。现如今的人工智能只有辅助功能，没有自主功能。目前的发展阶段，相当于当年蒸汽机火车刚推出的时候，离赶超人脑还非常漫长。

正在做的一些工作

Facebook发起Deepfakes检测挑战赛

在AI换脸盛行的背景下，9月6日，社交网络巨头Facebook宣布计划出资1000万美元，与人工智能（AI）合作伙伴、微软以及学术界一道发起DeepFake检测挑战赛。

Deepfake Detection Challenge

Deepfake Detection Challenge invites people around the world to build innovative new technologies that can help detect deepfakes and tampered media. Identifying tampered content is technically challenging as deepfakes rapidly evolve, so we're working together to build better detection tools.

Events Starting in October 2019

facebook

Microsoft

国家陆续出台自动驾驶安全标准

在政府报告中，最典型的是2016年美国政府发布的白宫报告《为未来人工智能做好准备》，美国政府认为人工智能越来越重要，美国需为未来做好准备，因此制定人工智能的发展路线和策略。

业界则有《阿西洛马人工智能原则》、谷歌人工智能原则等，其中发表于2017年1月阿西洛马人工智能原则尤为突出，此原则合计23条、分为“科研问题”“伦理道德”及“长期问题”三部分，倡议全球工业界、研究界采取措施共同保障人类未来的利益和安全。

我国对人工智能的发展也极为重视，近几年相继发布了《“互联网+”人工智能三年行动实施方案》《新一代人工智能发展规划》和《促进新一代人工智能产业发展三年行动计划》等一系列政策性文件，从战略层面引领人工智能发展。

最后

我推荐一个网站,里面详细的简介了deepfake的原理以及如何快速部署训练 deepfake.

!



<https://www.deepfakescn.com>

[参考文献]:

[如何建立法律领域的人工智能 悬赏1000万美元, 打假AI换脸! Facebook发起Deepfakes检测挑战赛 人工智能应用中的安全、隐私和伦理挑战及应对思考 如何确保人工智能的安全](#)