大家好，关于包括欧元很多朋友都还不太明白，今天小编就来为大家分享关于人工智能吗的知识，希望对各位有所帮助！

本文目录

2018年的人工智能行业的走向将会是怎样的？

据中研产业研究院发布的《2019-2025年中国人工智能行业发展分析与投资战略研究报告》统计数据显示

国际人工智能行业发展分析及经验借鉴

第一节全球人工智能市场总体情况分析

一、全球人工智能行业的发展特点

“人工智能”涵盖了很多前沿技术和分支，却很难用一句话来定义，因为它一直处在发展当中。比如，一些在过去看来很“人工智能”的事情，现在却变成了简单的“机械重复”，像是数字的高速计算、图像的处理等。但总体上来看，“人工智能”的本质和目的一直没有发生太多变化，那就是“完成人类的部分脑力工作”。

20世纪60年代开始，就有许多科幻电影和科幻小说描述着人类对“人工智能”的憧憬和恐惧，比如斯皮尔伯格的知名影片《人工智能》。不过在现实中，长久以来，受到技术、科技发展和应用层面的限制，人工智能只是一件人人都在说，都以为别人在做，但事实上却没多少人知道该怎么做的事——无论在学术研究层面还是在应用层面都是如此。

人工智能曾经在20世纪90年代互联网泡沫破裂前风靡一时，到了21世纪伊始却变成了一个禁忌，大家开始怀疑它是否存在。而到了2011年，美国资本市场再度为人工智能而疯狂。风险投资机构和顶级科技公司们开始频繁投资这个领域的创业公司，投资范围从应用层面的机器人、增强现实，到底层技术层面的深度学习算法、神经网络芯片等，人工智能项目也遍地开花。比如，Google接连投资了虚拟现实创业公司MagicLeap，收购了人工智能公司DeepMind;Facebook收购语音识别公司

Wit.ai，等等。

除了投资外部团队之外，像IBM、Google、Facebook和百度等国内外科技巨头们也纷纷加强自己的人工智能方面的专业团队，招募了一批人工智能尤其是深度学习相关领域的科学家，如深度学习鼻祖之一GeoffreyHinton加入了Google，YannLeCun加入了Facebook担任人工智能实验室负责人，AndrewNg(吴恩达)加入百度负责深度学习研究院等。

从人工智能的整个发展历程来看，按照应用场景和人工智能资源的集中度，可以大致分成三个阶段。

第一阶段：实验室研究阶段，这一阶段的人工智能资源高度集中。人工智能在2011年前的发展大致还处于实证研究阶段，资源高度集中在国家或大学资助的研究机构中，用于算法模型的训练和研究，人工智能还只能为极少数人接触到。这一阶段大量的工作除了在算法模型本身的研究外，还包括建立计算能力本身。

第二阶段：企业应用阶段，这一阶段的人工智能资源被少部分科技巨头掌握。在人工智能表现出一定的实际应用价值后，科技巨头们一拥而上，纷纷希望在这个领域取得突破。在少部分核心企业掌握了大规模的人工智能资源以后，其它小规模的企业一般会利用这些核心企业提供的人工智能资源接口和其支持的人工智能应用为自身的发展提供服务。由于掌握大规模的计算资源是这一模式的前提，因此这一阶段人工智能资源的集中度仍然非常高，而这将是人工智能在企业场景下的主要应用形式，即集中计算，分布使用。

第三步：个人应用阶段，这一阶段的人工智能资源被分散到个人手中。显然，依赖于云端大规模计算资源的人工智能算法限制着人工智能在消费者场景的应用，因为集中式计算意味着巨量的网络资源消耗，并且因为网络问题，难以在消费者应用场景中有稳定的表现。因此，人工智能的本地化，也就是从集中走向分布(细化到智能手机、可穿戴设备等)实现将是人工智能在消费者场景中得到普及的关键一步。伴随着人工智能的本地化实现，将使得人工智能真正延展到手持设备、家用电器、汽车等消费级应用。

图表：人工智能发展阶段

数据来源：中研普华产业研究院

二、全球人工智能市场结构

全球人工智能企业分布极不平衡，主要集中于美国、欧洲及中国等少数国家地区。

排名前三的美国旧金山/湾区、纽约及中国北京，企业数量分别占全球的16.9%，4.8%与4.0%。在增速方面，整体上一直保持增长势头，直至2015年出现小幅度回落。欧洲的人工智能企业多集中于本国家的首都。在欧洲各城市中，英国伦敦的企业数量最多，为第二位巴黎的3.1倍，占全球总数的3.69%。日本与韩国的企业数量明显不及中国，日本东京仅与杭州相当，韩国首尔仅与成都相当。东亚地区排名前三的城市，北上深三城占全球总数的7.4%。虽然还远不及美国，但在全球中的重要性将日益明显。

三、全球人工智能行业发展分析

“人工智能”涵盖了很多前沿技术和分支，却很难用一句话来定义，因为它一直处在发展当中。比如，一些在过去看来很“人工智能”的事情，现在却变成了简单的“机械重复”，像是数字的高速计算、图像的处理等。但总体上来看，“人工智能”的本质和目的一直没有发生太多变化，那就是“完成人类的部分脑力工作”。

20世纪60年代开始，就有许多科幻电影和科幻小说描述着人类对“人工智能”的憧憬和恐惧，比如斯皮尔伯格的知名影片《人工智能》。不过在现实中，长久以来，受到技术、科技发展和应用层面的限制，人工智能只是一件人人都在说，都以为别人在做，但事实上却没多少人知道该怎么做的事——无论在学术研究层面还是在应用层面都是如此。

人工智能曾经在20世纪90年代互联网泡沫破裂前风靡一时，到了21世纪伊始却变成了一个禁忌，大家开始怀疑它是否存在。而到了2011年，美国资本市场再度为人工智能而疯狂。风险投资机构和顶级科技公司们开始频繁投资这个领域的创业公司，投资范围从应用层面的机器人、增强现实，到底层技术层面的深度学习算法、神经网络芯片等，人工智能项目也遍地开花。比如，Google接连投资了虚拟现实创业公司MagicLeap，收购了人工智能公司DeepMind;Facebook收购语音识别公司Wit.ai等。除了投资外部团队之外，像IBM、Google、Facebook和百度等国内外科技巨头们也纷纷加强自己的人工智能方面的专业团队，招募了一批人工智能尤其是深度学习相关领域的科学家，如深度学习鼻祖之一GeoffreyHinton加入了Google，YannLeCun加入了Facebook担任人工智能实验室负责人，AndrewNg(吴恩达)加入百度负责深度学习研究院等。

图表：人工智能发展阶段

数据来源：中研普华产业研究院

从人工智能的整个发展历程来看，按照应用场景和人工智能资源的集中度，可以大致分成三个阶段。

第一阶段：实验室研究阶段，这一阶段的人工智能资源高度集中。人工智能在2011年前的发展大致还处于实证研究阶段，资源高度集中在国家或大学资助的研究机构中，用于算法模型的训练和研究，人工智能还只能为极少数人接触到。这一阶段大量的工作除了在算法模型本身的研究外，还包括建立计算能力本身。

第二阶段：企业应用阶段，这一阶段的人工智能资源被少部分科技巨头掌握。在人工智能表现出一定的实际应用价值后，科技巨头们一拥而上，纷纷希望在这个领域取得突破。在少部分核心企业掌握了大规模的人工智能资源以后，其它小规模的企业一般会利用这些核心企业提供的人工智能资源接口和其支持的人工智能应用为自身的发展提供服务。由于掌握大规模的计算资源是这一模式的前提，因此这一阶段人工智能资源的集中度仍然非常高，而这将是人工智能在企业场景下的主要应用形式，即集中计算，分布使用。

第三步：个人应用阶段，这一阶段的人工智能资源被分散到个人手中。显然，依赖于云端大规模计算资源的人工智能算法限制着人工智能在消费者场景的应用，因为集中式计算意味着巨量的网络资源消耗，并且因为网络问题，难以在消费者应用场景中有稳定的表现。因此，人工智能的本地化，也就是从集中走向分布(细化到智能手机、可穿戴设备等)实现将是人工智能在消费者场景中得到普及的关键一步。伴随着人工智能的本地化实现，将使得人工智能真正延展到手持设备、家用电器、汽车等消费级应用。

当前人工智能的浪潮已席卷了全球，人工智能领域的公司也在不断激增。根据VentureScanner的统计，截至到2016年初，全球共有957家人工智能公司，美国以499家位列第一。覆盖了深度学习/机器学习(通用)、深度学习/机器学习(应用)、自然语言处理(通用)、自然语言处理(语音识别)、计算机视觉/图像识别(通用)、计算机视觉/图像识别(应用)、手势控制、虚拟私人助手、智能机器人、推荐引擎和协助过滤算法、情境感知计算、语音翻译、视频内容自动识别13个细分行业。

四、全球人工智能行业竞争格局

各国政府高度重视人工智能相关产业的发展。自人工智能诞生至今，各国都纷纷加大对人工智能的科研投入，其中美国政府主要通过公共投资的方式引导人工智能产业的发展，2013财年美国政府将22亿美元的国家预算投入到了先进制造业，投入方向之一便是“国家机器人计划”。在技术方向上，美国将机器人技术列为警惕技术，主攻军用机器人技术，欧洲主攻服务和医疗机器人技术，日本主攻仿人和娱乐机器人。

现阶段的技术突破的重点一是云机器人技术，二是人脑仿生计算技术。美国、日本、巴西等国家均将云机器人作为机器人技术的未来研究方向之一。伴随着宽带网络

设施的普及，云计算、大数据等技术的不断发展，未来机器人技术成本的进一步降低和机器人量产化目标实现，机器人通过网络获得数据或者进行处理将成为可能。目前国外相关研究的方向包括：建立开放系统机器人架构(包括通用的硬件与软件平台)、网络互联机器人系统平台、机器人网络平台的算法和图像处理系统开发、云机器人相关网络基础设施的研究等。

由于深度学习的成功，学术界进一步沿着连接主义的路线提升计算机对人脑的模拟程度。人脑仿生计算技术的发展，将使电脑可以模仿人类大脑的运算并能够实现学习和记忆，同时可以触类旁通并实现对知识的创造，这种具有创新能力的设计将会让电脑拥有自我学习和创造的能力，与人类大脑的功能几无二致。在2013年年初的国情咨文中，美国总统奥巴马特别提到为人脑绘图的计划，宣布投入30亿美元在10年内绘制出“人类大脑图谱”，以了解人脑的运行机理。欧盟委员会也在2013年年初宣布，石墨烯和人脑工程两大科技入选“未来新兴旗舰技术项目”，并为此设立专项研发计划，每项计划将在未来10年内分别获得10亿欧元的经费。美国IBM公司正在研究一种新型的仿生芯片，利用这些芯片，人类可以实现电脑模仿人脑的运算过程，预计最快到2019年可完全模拟出人类大脑。

高科技企业普遍将人工智能视为下一代产业革命和互联网革命的技术引爆点进行投资，加快产业化进程。谷歌在2013年完成了8家机器人相关企业的收购，在机器学习方面也大肆搜罗企业和人才，收购了DeepMind和计算机视觉领军企业AndrewZisserman，又聘请DARPA原负责人ReginaDugan负责颠覆性创新项目的研究，并安排构建Google基础算法和开发平台的著名计算机科学家JeffDean转战深度学习领域。苹果2014年在自动化上的资本支出预算高达110亿美元。苹果手机中采用的Siri智能助理脱胎于美国先进研究项目局(DARPA)投资1.5亿美元，历时5年的CALO(CognitiveAssistantthatLearnsandOrganizes)项目，是美国首个得到大规模产业化应用的人工智能项目。Amazon计划在2015年能够使用自己的机器人飞行器进行快递服务。韩国和日本的各家公司也纷纷把机器人技术移植到制造业新领域并尝试进入服务业。

五、全球人工智能市场区域分布

图表：2018年全球人工智能企业数量前五名

数据来源：中研普华产业研究院

2018年，全球人工智能初创企业共计2617家。美国占据1078家居首，中国以592家企业排名第二，其后分别是英国，以色列，加拿大等国家。

全球人工智能企业融资规模的分布，与人工智能企业分布相同。美中英三国融资规

模为全球最大，但三者间的规模目前仍存在较大差距。

图表：2018年全球人工智能企业融资规模分布

数据来源：中研普华产业研究院

截止至目前，美国达到978亿元，在融资金额上领先中国54.01%，占据全球总融资50.10%;中国仅次于美国，635亿，占据全球33.18%;其他国家合计占15.73%。

中国的1亿美元级大型投资热度高于美国，共有22笔，总计353.5亿元。美国超过1亿美元的融资一共11笔，总计417.3亿，超过中国63.8亿。

六、国际重点人工智能企业运营分析

1、微软公司

(1)企业发展概况

微软，是一家美国跨国科技公司，也是世界PC(PersonalComputer，个人计算机)软件开发的先导，由比尔·盖茨与保罗·艾伦创办于1975年，公司总部设立在华盛顿州的雷德蒙德(Redmond，邻近西雅图)。以研发、制造、授权和提供广泛的电脑软件服务业务为主。

最为著名和畅销的产品为MicrosoftWindows操作系统和MicrosoftOffice系列软件，目前是全球最大的电脑软件提供商。

(3)微软AI研究新进展

微软在人工智能方面有着很深的积淀，比如微软研究院在语音识别、自然语言和计算机视觉、机器学习方面已经有很多成果，在这些研究的基础上微软先后推出了Skype即时翻译、小冰和小娜(Cortana)这样的AI产品。

而新成立的部门必将深化这种产研的结合。微软称，整合后的新部门将包括AI产品设计、基础与应用研究实验室，以及新体验与技术(NExT)这几部分。

而为了实现AI普及的目标，微软列出了4大重点关注领域：

代理。利用AI通过Cortana这样的代理从根本上改变人机交互方式。

应用。将智能注入从相机app到Skype、Office365等的一切应用。

服务。把注入到微软应用的相同能力(如视觉、声音等认知能力，机器分析能力)开放给全球的应用开发者。

基础设施。微软称要利用Azure开发出全球最强大的AI超级计算机并开放给每个人，让个人和组织都能利用它的能力(这让人想到IBM的Watson)

从中可以看出，微软已经把AI当作一种基础能力，希望从端到端渗透到各个领域。

(4)微软加快布局人工智能

现在，小娜(Cortana)收到的指令和问题已经超过120亿条，拥有1.33亿活跃用户。小娜可以在多设备上运行。她根据你的日常生活和工作养成的技巧，已经形成了一个高效的生态系统。通常在你意识到自己有需要之前，她就能做好准备。为了让开发人员都能够使用认知能力，微软还提供了CortanaIntelligenceSuite。

微软的MicrosoftPix应用是一个图片编辑工具，它能感知，帮助你选择合适的图像。

MileIQ是一个位置提醒APP，它的智能在于帮助你量化和分类旅行。SwiftKey是一个智能键盘，使用神经网络，根据你的输入方式进行训练，能为你想要输入的下一个词建模，即使这样一个简单的任务，也会变得更加智能。它不受平台的限制。SwiftKey现在已经被30亿安卓和IOS设备使用。在Office365中，MyAnalytics会追踪你每天的工作，通过图表展示你每天的时间分配。

客户关系管理(CRM)，CRM系统一般都是孤立的，用具体的术语为客户行动建模，为管理而建，而不是销售生产率。假如销售员能够根据客户的CRM系统之外的信息行动，比如来自Twitter，Facebook，客户服务应用程序等的信息，那会怎么样呢?微软在每天交互的应用中注入智能wait，可以让销售员以一种综合的方式采取行动，使用丰富的数据模型，这些模型能在所有的地方加入智能。

微软的平台BotFramework，允许在新的应用程序中建立智能的工具包——从Build大会以来，已经有40000开发人员使用它——包括像Uber这样的品牌，在认知服务中使用人脸识别APIs来改善他们的移动应用程序，以确保乘客安全。

AI服务需要各种类型的技术。为了实现这个目标，微软们已经往我们的云中投入大量FPGA(现场可编程门阵列)，它能直接与网络对话。在云中加入FPGA达到前所未有的网络性能，提高了所有工作负载的吞吐量，包括运行如SAP这种关键任务程序

。

此外，微软还有一个全球性的、超大规模的云基础框架，在云中增加了GPU，以提供更高性能的云接入，使一些从前根本不可能的方案得以实现。微软的Azure现在是世界上第一台AI超级计算机。

最后，还有研究AI的平台。微软支持所有的框架，其中，微软自己的CNTK是最快的分布式运算神经网络框架，也是唯一开源的可扩展的深度学习工具包。

(5)微软人工智能发展计划

2017年7月，微软宣布建立一个专注于人工智能的全新研究实验室MicrosoftResearchAI，EricHorvitz计划将不同的学科结合起来，以期创建更多通用的学习系统。

该新实验室将以位于华盛顿州雷德蒙德的总部为基础，由来自感知、学习、推理和自然语言处理等人工智能研究的多个子领域中的科学家组成。人数超过100人，约占微软研究院研究人员总数的十分之一。新的实验室系全球微软研究部门下属机构，微软雷德蒙研究院院长EricHorvitz同时担任MSRAI的负责人。

(6)、微软建立机器学习工具

无论是学术界的研究人员还是工业界的开发者，DMTK可以帮助他们在超大规模数据上灵活稳定地训练大规模机器学习模型。当前版本的工具包包含以下几个部分：

1.DMTK分布式机器学习框架：它由参数服务器和客户端软件开发包(SDK)两部分构成。参数服务器在原有基础上从性能和功能上都得到了进一步提升——支持存储混合数据结构模型、接受并聚合工作节点服务器的数据模型更新、控制模型同步逻辑等。客户端软件开发包(SDK)支持维护节点模型缓存(与全局模型服务器同步)、节点模型训练和模型通讯的流水线控制、以及片状调度大模型训练等。

2.LightLDA：LightLDA是一种全新的用于训练主题模型，计算复杂度与主题数目无关的高效算法。在其分布式实现中，我们做了大量的系统优化使得LightLDA能够在一个普通计算机集群上处理超大规模的数据和模型。例如，在一个由8台计算机组成的集群上，我们可以在具有2千亿训练样本(token)的数据集上训练具有1百万词汇表和1百万个话题(topic)的LDA模型(约1万亿个参数)，这种规模的实验以往要在数千台计算机的集群上才能运行。

想要了解更多关于行业专业分析请关注中研普华研究报告《2019-2025年中国人工智能行业发展分析与投资战略研究报告》

如何利用人工智能和传感器技术治理洪水？

据了解，英国每年都需要花费10亿英镑用于洪水管理，以避免气候变化带来的严重后果。近两年，英国谢菲尔德大学研究人员开发了一套借助物联网传感器和人工智能技术的CENTAUR系统，该系统使用人工智能技术来管理城市中的水流。通过传感器测得的数据，来帮助决定水应该如何流入人类住区和周围，以避免城市出现严重的洪涝灾害。

CENTAUR系统终端监测设备

据悉，该系统的工作原理是在下水道网络中安装“闸门”，可控制水从下水道网络的一个部分流向另一个部分。此外，还在上下游重点安装了水位传感器，以监测闸门两侧的水位。

该系统的目标是借助复杂的人工智能计算技术，结合特别设计的流量控制装置，在洪水风险高的特殊情况下，通过优化现有的管道内可用容量来衰减和储存水，从而在局部平衡洪水风险。

CENTAUR系统示意图

在极端天气情况下，闸门可进行远程控制，以防止重要地区发生洪水。例如，如果该系统网络的一部分开始向下游漫水，系统还可通过上游的水位传感器来检测水位上升，并关闭上游的闸门，从而减缓水流，或将其分流到有剩余容量的下水道的其他部分，从而防止水溢出街道。

据悉，该系统可通过人工智能技术实现完全自主，不需要中央控制。每个CENTAUR都将运行自己的本地传感器网络，传感器不仅用于通知本地控制，还将收集数据，使系统能够自我学习。

该系统成功应用于葡萄牙科因布拉市

目前，该系统已在葡萄牙科因布拉市和法国图卢兹成功进行了试用，且效果显著。因为该系统的成本相对较低，仅数万欧元，这意味着它可以很容易地纳入现有的城市防洪计划。不过，这一系统也有一个大的局限性，那就是如果城市下水道没有多余的储水容量，那么用人工智能的方式管理它们，将收效甚微。

延伸阅读：无锡借助物联网传感器技术实现智慧治水

近日，今夏首轮强降雨来袭，城市的排水管网系统迎来挑战。目前，在无锡市新吴

区智慧治水实时监控平台，该平台可对全区部分排水管网与河道安装上数据采集智能终端，以实现排水系统和水环境的精细化动态管理。

新吴区智慧治水实时监控平台

借助物联网传感技术和大数据的结合，在该平台运行的实时监控图上，可看到实时更新的地下管网“动态地图”。城市雨水、污水的管线、泵站、井口等节点运行数据，通过终端传感器设备的数据采集，全部数字化到GIS地图上。城市排水管网中流动的雨水和污水的实时状态、雨污合流溯源、排水用户超标排放、雨水管入河口水质等数据

AI时代无隐私，人工智能时代该如何保护隐私权？

我们处在一个智能变革的时代，人工智能技术正在“赋能”各行各业。大数据就像新能源，AI算法就像发动机，装载了大数据和人工智能技术的企业就像搭上了一班通往未来的快速列车，把竞争对手远远地甩在后面。

—

隐私

然而，这样的快速发展不是没有代价的。我们每个人的手机号、电子邮箱、家庭地址和公司地址经纬度坐标、手机识别码、消费记录、APP使用记录、上网浏览记录、搜索引擎结果的点击习惯、刷脸记录、指纹、心跳等等这些信息都是我们不愿意轻易给出的隐私数据，但在AI时代，这很可能已经成为某个公司用来训练AI算法的数据集中的一条。

正是众多不起眼的一条条个人隐私数据，构成了足够多的训练集，让AI从中学习到认知能力，让从未跟我们谋面的AI算法认识、了解我们，知道我们的喜好和动机，甚至还认识我们的家人、朋友。我们的隐私便是实现这些智能的“代价”。

当然，这个代价并不一定是你愿意拱手付出的。

那如何保护隐私？我不用行吗？

你以为关闭手机GPS就无法定位你的位置？你的手机还有陀螺仪、内置罗盘、气压计等装置，还是可以用来定位你的位置。只要使用手机，就不存在绝对的隐私保护。

对于很多手机应用来说，要么不用，用了就很难避免泄露隐私，比如很多APP必须用手机号注册，或者需要手机验证才能继续使用，还有的需要刷脸验证等等。那么，个人想保护隐私能做什么？什么也做不了，加上AI算法的黑盒性质，我们甚至对于AI背后的逻辑和动机一无所知。

—

监管

隐私保护靠个人防护真的很难实现，需要强有力的法律法规来限制。

2018年5月25日，欧盟的《通用数据保护条例》（GDPR）正式生效，这是在欧盟范围内的一个数据保护监管框架，这是目前最完善、最严格的隐私保护规定。根据DLAPiper公布的数据，在不到两年的时间内，GDPR已产生1.14亿欧元的罚款，其中开出的最大罚单是法国依据GDPR对谷歌罚款5000万欧元，理由是谷歌在向用户定向发送广告时缺乏透明度、信息不足，且未获得用户有效许可。下图是GDPR生效以来至2020年1月份欧盟各个国家罚款的金额分布图。

对于企业，GDPR要求在收集用户的个人信息之前，必须以“简洁、透明且易懂的形式，清晰和平白的语言”向用户说明将收集用户的哪些信息、收集到的信息将如何进行存储、存储的信息将会被如何使用，并告知企业的联系方式。

对于个人，GDPR赋予数据主体七项数据权利：知情权、访问权、修正权、删除权（被遗忘权）、限制处理权（反对权）、可携带权、拒绝权。目前GDPR在真实地影响到我们每个人的生活，最直观的影响就是当你浏览网页的时候，你会发现经常遇到网站弹出类似下图的提示，这是网站基于信息透明性的规定，向你征询信息收集的许可。

欧盟的GDPR具有全球影响力，它让用户对自己的个人数据有绝对的掌控权，让全球在发展新技术的同时必须开始关注隐私问题，世界各国已经纷纷出台自己的数据保护法规。

关于隐私保护，一切才刚刚开始。

欧盟在上个月正式启动了称为“打造欧洲数字未来”的新战略，打算通过制定一系列针对AI、隐私和安全的法规，成为AI发展的全球领导者。该战略的启动也被看成是在应对美国和中国的AI崛起。

可以预见，关于AI的隐私安全与监管将逐渐成为重点话题，实际上，就像欧盟委员

会副主席MargretheVestager说的：“人工智能本身并没有好坏之分，而是完全取决于人们为什么以及如何使用它。让我们尽可能做到最好，控制人工智能可能给我们的价值观带来的风险——不伤害，不歧视。”

保护隐私已经成为AI发展不可绕过的“槛”，是AI技术的难题，也是AI良性发展的契机。

三

趋势

可以说，保护隐私的各种法规的出台必然是未来不可避免的趋势，这势必让企业的数据收集、使用及流通的合规成本大幅增加，也容易让企业内部或者企业间形成数据孤岛问题，制约企业获取数据价值。因此，保护隐私的AI技术的落地使用成为AI领域最亟待实现的目标。

保护隐私的AI主要通过数据加密、分布式计算、边缘计算、机器学习等多种技术的结合来保护数据安全，近期比较热门的有DifferentialPrivacy（差分隐私）、FederatedLearning（联邦学习，也叫联盟学习、联合学习、共享学习）。

保护隐私不是说完全不收集数据，而是要通过技术的手段防止个人隐私数据的泄露。差分隐私是一种数学技术，比如，假设要分析数据集并计算其统计数据（例如数据的平均值、方差、中位数、众数等），如果通过查看输出，我们无法分辨原始数据集中是否包含了任何个体的数据，那么这种算法就被称为差异私有。

举个非常简单的例子，假设你的工作部门每个月都会用一个表格统计部门每个人的工资发放金额，除了制表人，别人无法查看这个表格，只能通过一个查询函数S知道这个表的总额，某个月你调去了别的部门，那么别人就可以通过上个月表格A，和这个月表格B来知道你的工资，道理很简单，只需用S(A)减去S(B)。B表格称为A表格的相邻数据集，它俩只相差一条数据，差分隐私技术就是要让相邻数据集的查询结果差不多，从而无法推出个人的信息来，这个差不多的程度可以看作隐私保护的力度。苹果和Facebook已经使用这种方法来收集聚合数据，而不需要识别特定的用户。MITTechnologyReview将差分隐私技术列为2020全球十大突破性技术之一。

联邦学习采用了分布式机器学习方法，近年来越来越受欢迎，该技术假设用户数据不会被存储到中心化的服务器，而是私有的、保密的，仅存储在个人的边缘设备上，比如手机，因此与传统机器学习方法相比，联邦学习从根本上增强了用户隐私。联邦学习不依赖从用户设备端收集的数据来训练，而是在用户移动设备端训练AI模

型，然后将训练得到的参数信息传输回一个全局模型，这个过程不需要用户数据离开个人设备。

从近两年在arXiv（一个提交论文预印版的平台）上提交的论文数可以看出，该技术发展的快速趋势：

四.巨头的技术布局

从去年起全球最流行的两个机器学习框架，TensorFlow和PyTorch都增加了联邦学习等解决方案来保护隐私。

（1）Google

联邦学习的概念最早是由Google在2017年首次引入，去年又发布了TensorFlowFederated（TFF）框架，利用Tensorflow的机器学习框架简化联邦学习。

如下图所示，基于TFF框架搭建的学习模型在众多手机（如手机A）上进行本地化模型训练，更新权重并聚合（步骤B），进而更新提升后的全局模型（模型C），将全局模型再应用到各手机终端来提升算法应用效果。

2）Facebook

为了在保护隐私的机器学习领域取得进展，去年Facebook旗下优秀的深度学习框架PyTorch与OpenMined宣布开发一个联合平台的计划，以加速隐私保护技术的研究。

OpenMined是一个开源社区，专注于研究、开发和升级用于安全、保护隐私的AI工具。OpenMined发布了PySyft，是第一个用于构建安全和隐私保护的开源联邦学习框架。

PySyft很受欢迎，在Github已经拥有5.2k个Star，目前支持在主要的深度学习框架（PyTorch、Tensorflow）中用联邦学习、差分隐私和加密计算（如多方计算，同态加密），实现将隐私数据与模型训练解耦。

五国内发展现状

国内的AI巨头们也早已开启保护隐私的技术布局，特别是金融领域，金融领域由于监管严格，数据的隐私性要求极高，因此，金融机构一方面在保护隐私数据方面面临技术难题，另一方面由于金融数据的孤立性，“数据孤岛”问题导致金融机构无

法发挥出数据的真正价值。

国内多家金融机构以及金融科技公司已经尝试在获客、授信、风险控制等方面，利用联邦学习解决数据隐私的合规问题和数据分享的数据孤岛问题，最大化的发挥金融数据价值。

目前国内关于保护隐私的监管还不够成熟，个人和企业对于隐私保护的意识还不强。随着全球环境中对保护隐私的关注逐渐加强，以及保护隐私的AI技术的发展，我相信AI技术终究会向着更好的方向发展，希望通过科学家们的努力，AI的黑盒不会是潘多拉之盒。

现在我们所说的人工智能，和10年前提出的“人工智能”概念有什么不同？

人工智能是计算机科学的一个分支，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器，该领域的研究包括机器人、语言识别、图像识别、自然语言处理和专家系统等。人工智能从诞生以来，理论和技术日益成熟，应用领域也不断扩大，可以设想，未来人工智能带来的科技产品，将会是人类智慧的“容器”。人工智能可以对人的意识、思维的信息过程的模拟。top域名认为人工智能不是人的智能，但能像人那样思考、也可能超过人的智能。

OK，本文到此结束，希望对大家有所帮助。