AI精度与隐私的博弈

AI Time 第十五期

本期Contributors: 北京智源人工智能研究院

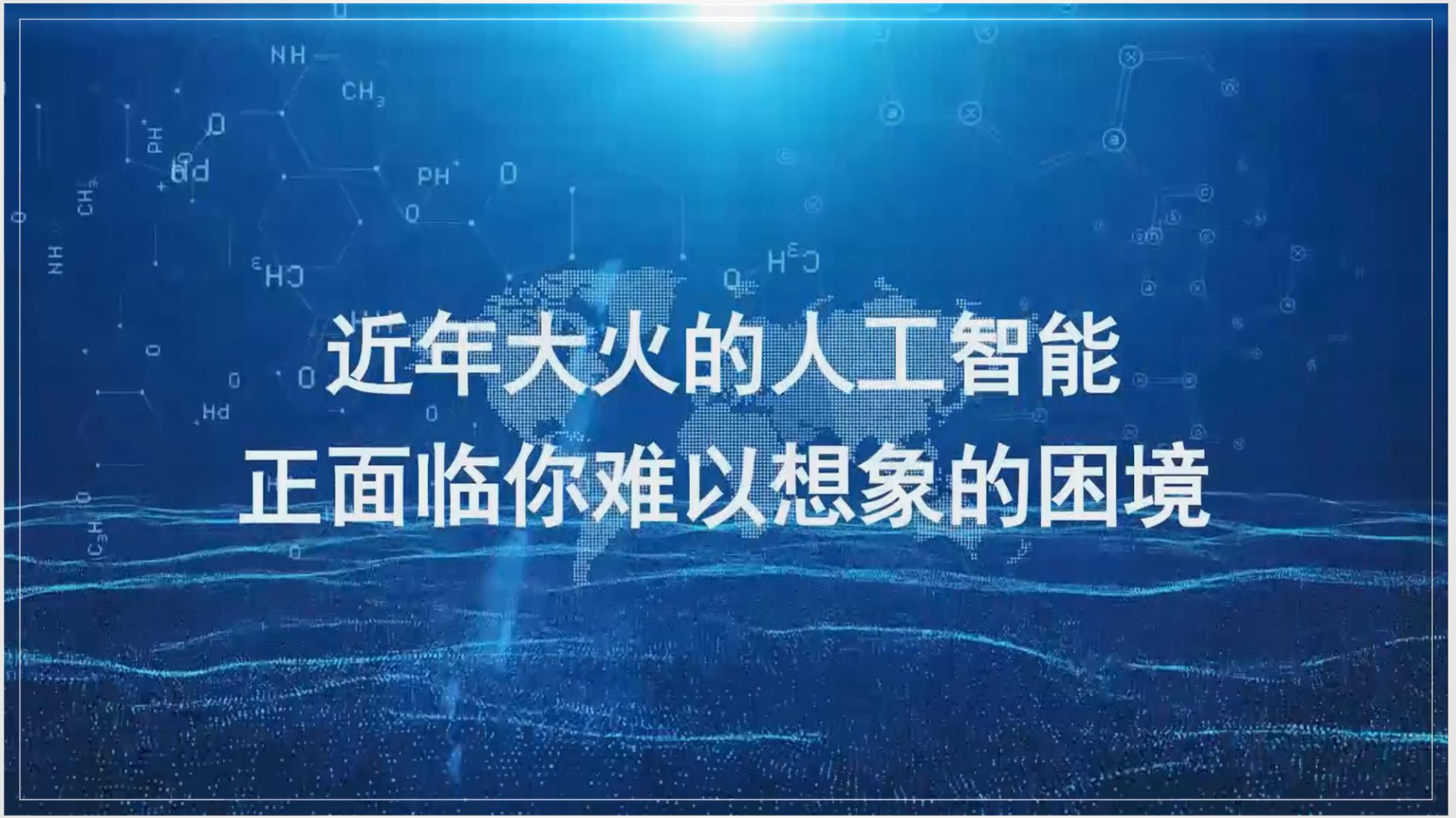
AI Time、微众银行

AI Time是一群关注人工智能发展，并有思想情怀的青年人创办的圈子。AI Time旨在发扬科学思辨精神，邀请各界人士对人工智能理论、算法、场景、应用的本质问题进行探索，加强思想碰撞，打造成为北京乃至全国知识分享的聚集地。

序言

AI的发展以大数据为驱动，在跨区域跨组织的大数据与AI协作需求愈发迫切的当下，随着科技的发展，关于数据隐私与安全的话题，受到大众广泛关注。

AI时代，大众真的“无隐私”吗？以“联邦学习”为代表的新兴AI技术能否实现AI协作，提升模型精度的同时，实现数据隐私保护？中国如何抢占人工智能安全发展的制高点？下一个十年中，人工智能将何去何从？


近年大火的人工智能
正面临你难以想象的困境

嘉宾介绍

张钹

中国科学院院士

智源研究院学术顾问委员会委员

高文

中国工程院院士

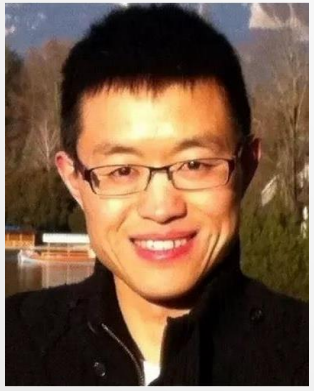
智源研究院学术顾问委员会委员

杨强

香港科技大学讲席教授

微众银行首席人工智能官（CAIO）

主持人



唐杰

智源研究院学术副院长

清华大学教授

刘知远

清华大学副教授

智源青年科学家

议程

- AI当前面临的挑战
- 圆桌讨论：
  1）数据隐私之忧
  2）技术突围之道
  3）下一代人工智能
- 总结与展望

人工智能核心进展停滞不前?

SHARE

IN DEPTH | COMPUTER SCIENCE

Core progress in AI has stalled in some fields

Matthew Hutson

+ See all authors and affiliations

Science 29 May 2020:
Vol. 368, Issue 6494, pp. 927
DOI: 10.1126/science.368.6494.927

Article | Figures & Data | Info & Metrics | eLetters | PDF

You are currently viewing the summary.

View Full Text

Science
Vol 368, Issue 6494
29 May 2020

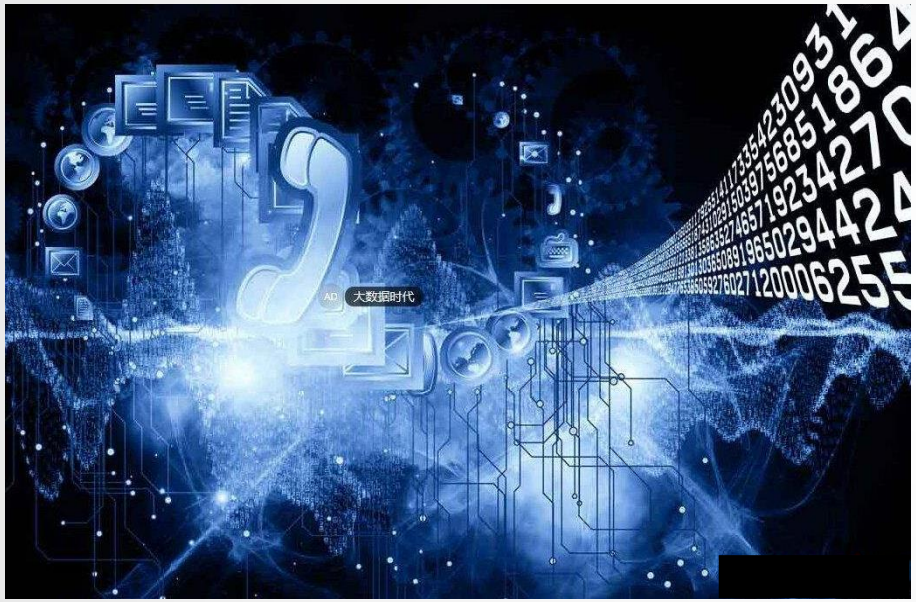
Table of Contents
Print Table of Contents
Advertising (PDF)
Classified (PDF)
Masthead (PDF)

ARTICLE TOOLS

Email
Print
Alerts
Share
Download Powerpoint
Citation tools

MY SAVED FOLDERS

大数据： 理想与现实



个人隐私与数据法规： 欧盟的 GDPR

- 《通用数据保护条例》（General Data Protection Regulation，简称GDPR）为欧盟于2018年5月25日出台的条例。
- 对违法企业的罚金最高可达2000万欧元（约合1.5亿元人民币）或者其全球营业额的4%，以高者为准。
- 网站经营者必须事先向客户说明会自动记录客户的搜索和购物记录,企业不能再使用模糊、难以理解的语言，或冗长的隐私政策来从用户处获取数据使用许可。
- 明文规定了用户的“被遗忘权”（right to be forgotten），即用户个人可以要求责任方删除关于自己的数据记录。

2018年5月28日报道：
Facebook和谷歌等美国企业成为GDPR法案下第一批被告。

GDPR下，IT巨头纷纷被罚

French regulator fines Google $57 million for GDPR violations

Share on Facebook Share on Twitter +

Google hasn't transparently implemented GDPR rules, French regulator claims.

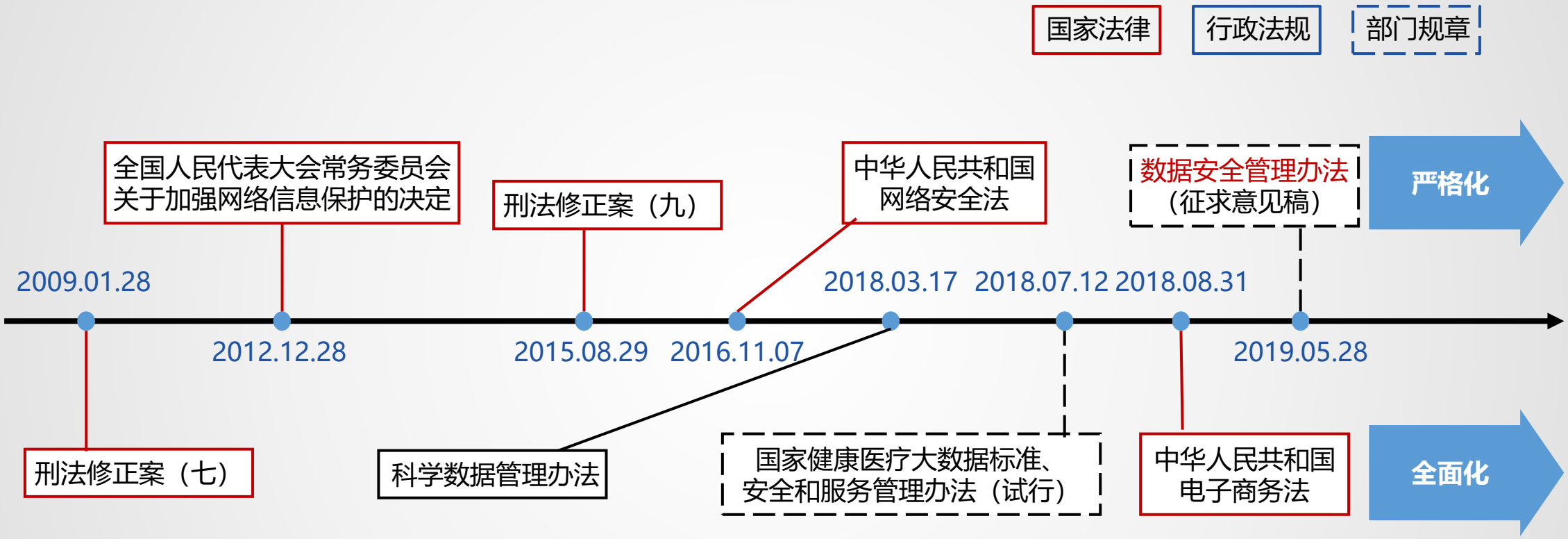
1 . France's National Data Protection Commission (CNIL) found that Google provided information to users in a non-transparent way.

"The relevant information is accessible after several steps only, implying sometimes up to 5 or 6 actions" - CNIL said.

2. The users' consent, CNIL claims, "is not sufficiently informed," and it's "neither 'specific' nor 'unambiguous'."

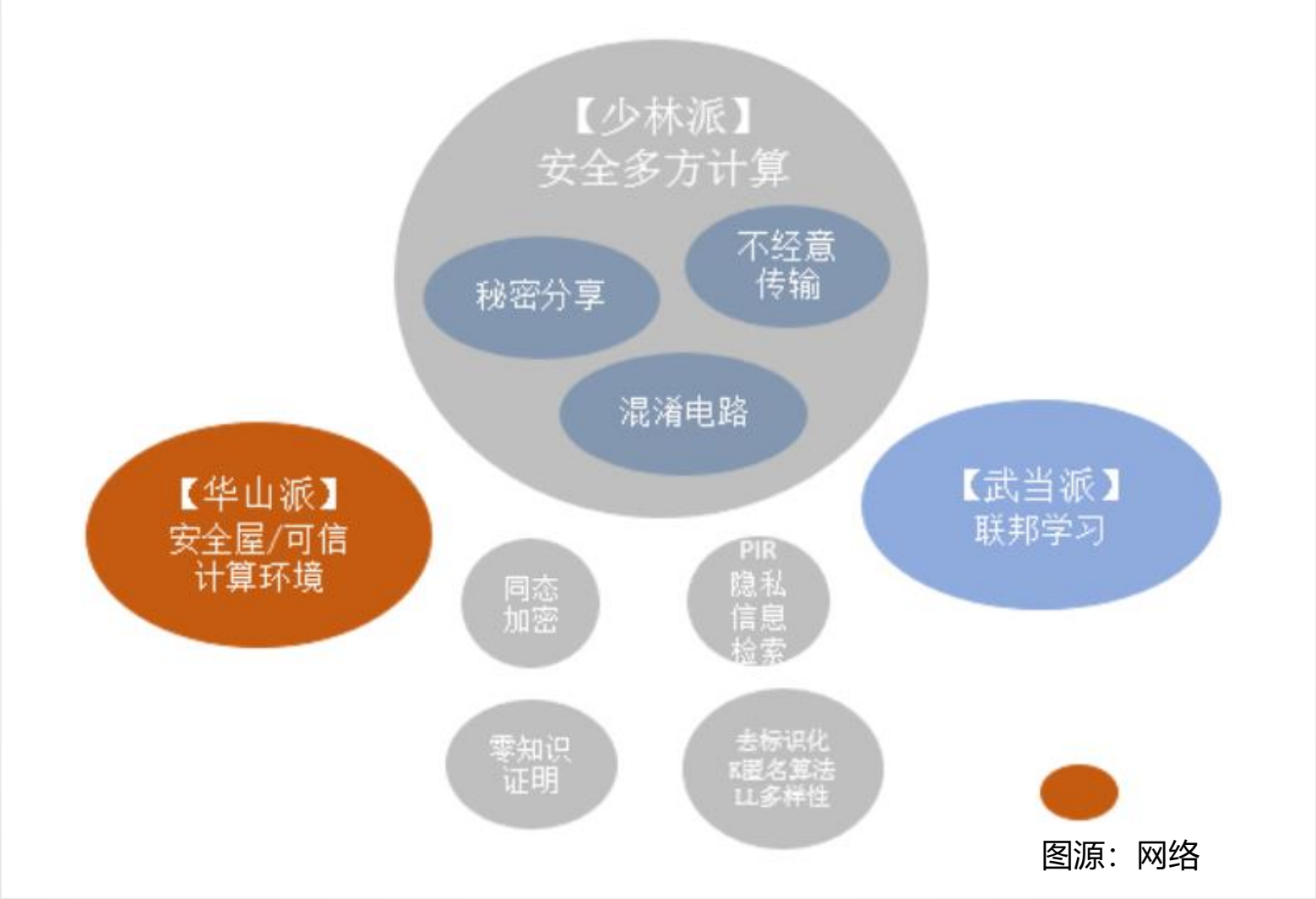
To date, this is the largest fine issued against a company since GDPR came into effect last year.

国内的数据监管法律趋严



严格化：数据控制方责任明确，刑罚到自然人
全面化：各领域数据管理细则密集出台，用户授权+监管部门审批

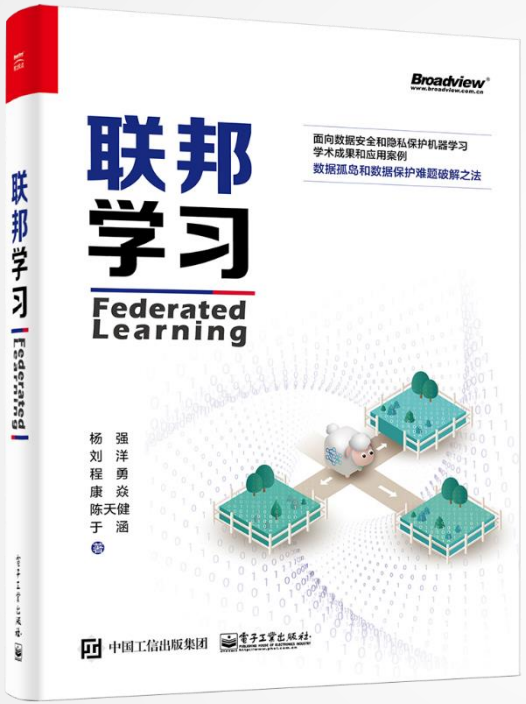
技术破局——隐私计算技术的三大主流门派

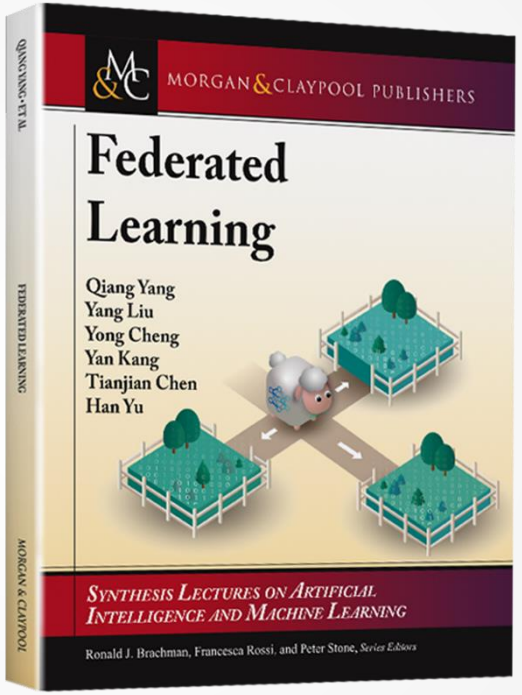


图源：网络

技术破局——联邦学习

技术破局——联邦学习





世界第一本联邦学习专著

思辨与讨论

思辨与讨论

1）数据隐私之忧

2）技术突围之道

3）下一代人工智能

思辨与讨论

数据隐私之忧

- 提升模型精度是否一定意味着牺牲隐私保护？美国多地禁止人脸识别，重视隐私保护是否阻碍人工智能发展？
- 对AI应用的用户隐私与数据安全的担忧是杞人忧天还是未雨绸缪？
- 如何处理好发展AI技术（比如提升模型精度，实现认知智能）与人的关系？

思辨与讨论

技术突围之道

- 以联邦学习为代表的AI新技术能否解决大数据AI协作与数据隐私保护之间的矛盾?
- 这些技术的优势与局限性有哪些?
- 如何让更多人参与到这些技术创新中来，开源？激励机制?

思辨与讨论

下一代人工智能

- 下一代人工智能技术应该具备哪些特点?
- 我们如何抢占制高点?

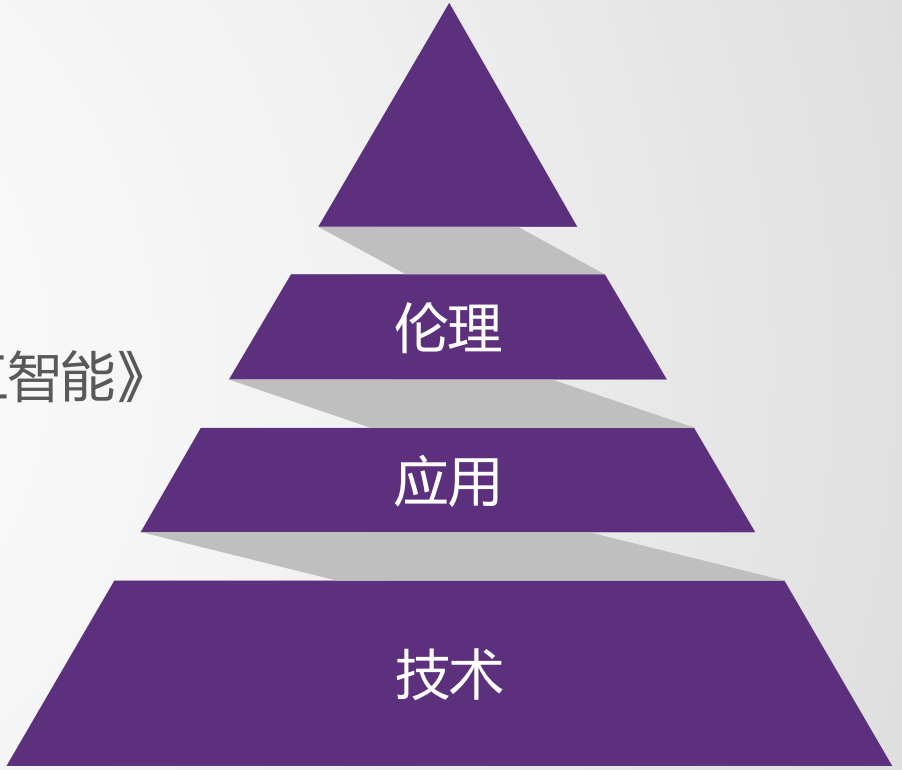
总结与展望

AI的下一个十年

负责任的AI

国家新一代人工智能治理专业委员会：

《新一代人工智能治理原则——发展负责任的人工智能》



人与AI的协作

人与AI如何更好地协作，创造更大价值

谢谢大家

AI Time欢迎每一位有情怀的AI爱好者加入！我们需要您的思辨和碰撞！