CBINSIGHTS | CHINA

2022年中国隐私计算技术与市场发展研究报告

CBINSIGHTS | CHINA

目录

导语

数字时代的智慧应用与数据密不可分，数据作为底层资源喂养了庞杂算力体系下的各类智能算法。然而近年来数据利用面临越来越多挑战，也因挑战逐渐生变。

首当其冲的是数据隐私问题，数据隐私日渐从社会讨论、传媒声势中落地。在顶层设计方面，事关数据隐私的法律法规逐步完善；在技术上，诸如同态加密这类隐私计算技术已经深入人们日常生活，在手机等智能设备中以难以察觉的方式落地应用。

其次，数据智能的逻辑为数据喂养算法，应用的智能程度与数据的量和质有着莫大因果关联。而随着智能应用的发展阶段不断推进、综合智能程度提升，智慧应用更需要开辟新渠道拓展数据类型，利用优质多维度的丰富数据全面提升智能程度。

隐私计算行业的勃兴正是在此背景下涌现的一波技术商业化浪潮。在技术方面，隐私计算实质上并不指实际的单个技术，而是囊括了多个技术类别的一揽子技术合集。“隐私”为目的项，指明了技术本身功用乃是达成隐私保护。而“计算”则说明了该技术在本质上是对信息、数据的加工，即应用在数据的使用流程中。

隐私计算以“数据可用不可见”切入数据使用过程，最终达到打通“数据孤岛”的目的。这带来了两方面的益处。其一，“可用不可见”某种程度上绕开了数据权属争议，通过技术手段保证了原始数据归属于某一方，与此同时将使用权分离出来，通过平台及技术进行交易、释放数据。其二，数据孤岛的根源在于数据权属问题、数据隐私问题等多重因素交织。因数据有易复制、易篡改特质，所有权难以界定。隐私计算保证数据归属清晰的同时挖掘数据价值，与此同时有效保障了数据内容中包含的隐私信息不被泄露，在涉及个人身份信息及某些特殊场景下具有重要意义。

导语

随着中国的《数据安全法》、《个人信息保护法》等数据监管法律相继在 2021 年落地，数据利用面临更多制约因素，数据合规成为行业数据利用大考。与数据监管相伴的仍旧是数据赋能数字经济的逻辑，只有持续挖掘海量数据才能不断升级应用智慧程度，从而促进数字经济和智能经济发展，最终变革社会、惠及社会。

以此为背景，近年来围绕数据要素涌现了一个全新的数据服务市场，在政策鼓舞下有着清晰的发展持续性，大数据中心在中国各地分级有序建设，数据交易所不断涌现。而隐私计算作为赋能数据利用流程的核心技术之一，将成为数据服务市场的底层基础设施，为数据交易创造条件并守护数据隐私。简言之，隐私计算在近两年迎来了风口，并将会在眼下数据服务市场中占据牢固位置，以技术赋能市场要素市场建设。

通过文献研究与产业调研，本报告理解掌握行业重点问题、呈现行业全景：阐明行业发展背景、追索技术发展历程、描绘行业玩家图谱、研判未来发展趋势：

第 1 章“掘金”：从价值落实、监管加强、技术进展等维度出发得出结论，隐私计算在本质上是数字经济发展到一定阶段必然需求，该技术能响应价值、顺应监管、赋能技术；

第 2 章“利器”：从技术属性出发，追溯隐私计算技术的发展脉络与特征；

第 3 章“索骥”：描画现有隐私计算公司图谱，依据各自资源与特征，概括为四种主要玩家，并进一步探究相关玩家的主流商业案例；

第 4 章“乘势”聚焦商业化现状及研判市场机会点，指出当下正在积极建设中的数据要素服务市场是隐私计算面临的持续机遇。

Chapter 1

掘金：

新型生产要素数据迎来政策红利，隐私计算顺势而为

- 底层价值：应对长期潜伏的数据隐私与安全挑战
- 强化监管：促进数据合规利用，守护基本价值
- 技术增益：隐私计算技术蓬勃发展，为数据合规提供技术支持
- 市场回响：隐私计算赛道投融资势头强劲

底层价值：应对长期潜伏的数据隐私与安全挑战

数据价值开始深入政策层面，由此传导到业界愈加彰显，同时合规的数据流通程序也将为数字经济生产赋予更明晰、更广阔的发展空间。

在 2021 年 4 月公布的《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》中，数据被定义为生产要素且与“土地、劳动力、资本、技术”并列，数据对于国民生产的重要价值得到了官方层面肯定，且重要程度一举提升到了与其他基本要素同等地位。

数据的生态全流程大致可分为存储、传输、使用三大环节，在数据的传输和使用过程中，由于数据主体的差异，往往涉及到事关个体的隐私问题以及事关企业主体的数据安全问题。

1.数据隐私：避免侵蚀个人权益，有效保全经济和人身利益

究其本质，基本隐私权利在于不被观察、监视的权力。保障个人隐私，即是保障了个人自如行动的基本前提。在隐私得以保全的前提下，人可以相对自如地按照自身需求、兴趣和利益作出相应的行动，达成相应目的。在具体形式上，人们拉窗帘、戴墨镜、避人耳目私底下交谈都在为自如活动创造了机会。

在大数据时代，个人更需要免于被商业机构的“数据监控”，免于被追踪、分析，进而免除经济甚至人身安全侵犯。在此背景下，“大数据杀熟”案例层出不穷，部分商家利用各类渠道搜集用户信息，侵害用户隐私。在典型案例中不法商家获取到消费者全面画像，依照个体收入水平等特征提供“水涨船高”的价格，由此获取了额外利润。

底层价值：应对长期潜伏的数据隐私与安全挑战

在商家侧，所取得的额外利益建立在侵害隐私、获取数据的前提上。在用户侧，客户隐私被侵害后便丧失了部分自主行动权，失去了本可依照价格做出符合利益兴趣的合理决策，但在获取到量身定制的混淆信息后，无法维护自身利益。

根据 IBM 报告《Cost of a Data Breach Report 2021》，个人可识别信息（ PII, 指的是可用来辨识某人身份的信息）在所有数据泄露中占比高达 44%，单个信息泄露会给相关企业造成高达 180 美元的成本。在宏观层面，报告所涉企业案例中，当泄露信息量在 5000 万–6500 万条区间时，单个企业平均处理成本达到了约 4 亿美元。从数字不难看出，隐私泄露每年实际造成了大量经济损失[1]。

当下的数据已经呈现了如下特征：

数据总量与维度愈加丰富：数据已经从模糊化、碎片化，逐渐变得清晰化、完整化。在金融服务、出行、政务、娱乐等诸多维度各方面信息的汇聚下，数据关涉的个人画像越来越清晰。

数据触角深探个人生活：数据可描绘的个人画像逐步深入，从无关痛痒的外在场景化消费信息，变为直指个人身份的关键依据。以医疗数据为例，随着医疗系统的数字化以及数字化医疗渐成大势，个人外在身份、既往疾病信息、体内指标等数据足够勾勒出细微信息，数据深入了更为隐秘的角落。

在现今的数据维度下，一旦有企业个体出于特定目的汇集金融、出行、医疗等多维数据，牵涉的数据主体的隐私将暴露无疑。对于大数据时代的数据主体而言，隐私问题早已是重大风险项。

[1] IBM. *Cost of a Data Breach Report 2021*. https://www.ibm.com/security/data-breach.

底层价值：应对长期潜伏的数据隐私与安全挑战

案例

Vastaamo 公司数据泄露事件

2020 年，芬兰心理健康服务平台 Vastaamo 发生大规模数据泄露事件。

由于该公司系统安全漏洞，4 万多个客户的基本信息和医生诊疗的手账全部落到黑客手中。其后，多达 300 多个客户的资料被黑客分批泄露到暗网中，黑客直接在网络上要挟分批次释放客户信息，名单上的客户若不及时满足他们索要的金额便将之公之于众。

其后黑客分批次将其完全暴露在网上，包含客户诊疗时真实记录等信息曝光，部分客户隐秘角落被迫公之于众。泄露信息囊括了医生详细的问诊手记，如实记录病人病理情况诸多细节。作为医疗数据，事件影响直抵个人，并对平台造成了决定性的破坏影响。

泄露开始于 2020 年 10 月，仅仅数月之后的来年 2 月，历经两轮融资、有近 400 人团队的 Vastaamo 宣告破产。

对用户而言这起事件无疑是一场灾难，个人名誉收到严重侵害，而同时对其他公司也敲了一记响亮的警钟，提醒业界公司重视客户隐私和数据安全[2]。

2.数据安全：支撑数字经济的基层价值底座

数据安全指的是个人或机构的数据免于外界未经授权的滥用、盗用行为，及自然灾害、技术问题带来的个人和机构的兴趣利益受侵犯的安全。根据 2021 年 6 月通过的《中华人民共和国数据安全法》：“数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。”

在数据安全实践上，据著名数据安全商 RBS 统计，2020 年据公开渠道统计共有近 4000 起相关信息泄露事件使个人处于受威胁的状态中。此外海量商业机密也将使机构蒙受可能损失[3]。

[2] Ralston, W. *They Told Their Therapists Everything. Hackers Leaked It All.* WIRED. https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/
[3] RiskBased Security. (2020). *2020 Year End Report Data Breach QuickView.*

底层价值：应对长期潜伏的数据隐私与安全挑战

3.数据隐私与数据安全：相互交织，共同构成数字经济价值底座

数据安全是数据存储、传输、使用三大环节中最重要底层安全之一。数据隐私则是在数据安全之上发展性价值。两者的在概念上具有交叉部分、实践过程中也常常关联在一起。如果数据安全缺乏保障，在国家层面数据主权将无从建立，在机构和个人方面则基本利益将受到侵害。

数据安全是数据的基础性需求，只有数据安全得以保障，数据存储、传输、使用的任一流程、任一主体才能自如参与全链路，以数据达成自己的利益兴趣。而数据隐私则是建立在数据安全基础之上的数据价值理念，在层级上比数据安全更高，在时间发展先后性上，往往只有当基层建设（也即数据安全）达成一定程度的成功后，才逐渐浮现。

两者关系密不可分，主要表现在数据隐私的前提是数据安全。只有数据无法被非法第三方截取、篡改、非法持有，数据的隐私才得以保障。根据数据安全伦理研究学者意见，数据的基础价值有数据安全、数据隐私、数据平等和数据可问责四项基本内容。与数据安全相比，数据隐私往往体现为发展性需求。

隐私问题在近几十年重视程度不断加深，从宏观的法律法规导向到社会舆论兴起，最后才是推动了商业机构的拓展落地。与之类似，中国的隐私问题在近年来在多方的注视下从理论上落地现实，相关话题从懵懂的意识、社会讨论、共识逐渐生成，最终到立法机构推动、行业标准形成、约束机制等方面落地。

强化监管：促进数据合规利用，守护基本价值

1.以欧洲 GDPR 法规为代表，世界范围内数据监管力度加强

欧洲作为隐私保护先驱，制定具有开创性的指令与法律：在世界范围内，数据隐私相关法律法规最早可追溯至以《通用数据保护条例》（GDPR）为线索的欧盟系列规定。

早在 1995 年，欧盟就通过了《数据保护指令》（Data Protection Directive），明确规定了最低的数据隐私与数据安全底线标准。该指令为法律框架而非主权国家法律，需要转为欧盟成员国的法律从而生效，为各个国家自行落实。因此在约束力层面与法律难以相提并论。

随着以互联网为代表的新兴数据载体崛起，数据隐私与数据安全迎来新的挑战。在 2011 年，谷歌公司为精准推送广告擅自扫描用户的邮箱内容，因侵犯用户隐私被告上法庭。由该案延伸出的数据隐私、数据确权问题引起了广泛讨论。自此欧盟逐渐意识到“需要全面深刻的保护个人隐私方式”，于是开启了对《数据保护指令》更新工作。到 2016 年，欧洲议会正式通过《通用数据保护条例》并生效。从 1995 年的“指令”升级为 2016 年的“条例”以法规形式对欧盟成员国产生直接约束作用。到 2018 年5 月，该法规正式全面落地欧盟所有机构[4]。

《通用数据保护条例》规定了包括“目的限定”（数据搜集仅出自特定目的）、“数据最小化”（严格限定搜集的数据量）、“正当与负责”（确保数据安全、正当、保密，可动用加密机制）的基本原则，在数据隐私方面法规中具有领先的指导意义。而在 2018 年，美国加州通过了《加利福尼亚州消费者隐私保护法案》（CCPA），该法案一定程度上承接了欧洲 GDPR 的部分精神，规范企业如何处理消费者的个人信息。

[4] GDPR.EU. *What is GDPR, the EU's new data protection law?* https://gdpr.eu/what-is-gdpr/

强化监管：促进数据合规利用，守护基本价值

中国近年来陆续出台重要法律，逐步完善框架、守护隐私：在中国，与数据隐私、数据安全相关的法律法规主要有三部：分别为 2017 年生效的《网络安全法》、2021 年 9 月生效的《数据安全法》和 2021 年 11 月生效的《个人信息保护法》。三部法律共同确立了中国数据隐私、数据安全的法律框架主体，分别在网络安全管理、数据安全与发展、个人信息处理权利义务等领域做了界定与规定，使得数据流转的安全、隐私有法可依。

其中，《个人信息保护法》被部分媒体称为最为严格的个人信息保护法律法规。在基本的内容上，该法承接了上述几个法律法规文档部分精神，限定了目的的正当性，搜集个人信息目的的明确性，以及搜集的数据量限定于能直接服务于目的的最小范围。

国家/地区	法律法规	生效时间
中国	《网络安全法》	2017.06
	《数据安全法》	2021.06
	《个人信息保护法》	2021.11
欧洲	《关于个人数据处理保护与自由流动指令》	1998.10
	《数据保护通用条例》	2018.05
美国	《加州消费者隐私法案》	2018.06
加拿大	《个人信息保护和电子文件法》	2001.01
日本	《个人信息保护法》修改法案	2020.06

表 | 主要国家/地区的隐私相关法律法规（来源：CB Insights 中国）

强化监管：促进数据合规利用，守护基本价值

2.监管精神：厘清合规条例，促进数据经济要素的自由流转

作为重要性日益凸显的经济要素，数据只有在合理地流动中才能产生相应的价值。因此，对数据隐私的加强保护并不等同于弱化数据流动。相反，从各国的法律法规中，都能见到促进数据在合规前提下，强化数据价值的相关精神体现。

在欧洲的《通用数据保护条例》中，序言第 26 条指出：数据保护原则不适用于匿名化的信息，也即不适用于非身份数据。同时，若个人信息数据已匿名化处理且不再可识别身份，同样不适用该原则、法律。因此，出于统计或研究目的并经过匿名化处理的信息，该法并不适用[5]。

而《中华人民共和国个人信息保护法》明确规定“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。” 其中，“匿名化处理后的信息”不属于匿名信息，在保护隐私的前提下，为各种数据应用打开了窗口。在该法的第五十一条中，明确了可以“采取相应的加密、去标识化等安全技术措施”从而使得个人信息处理过程合法合规，防止个人信息的泄露、篡改和丢失[6]。

由上述法律法规的精神与细则可以看到，数据隐私方面的相关顶层设计无不在隐私与利用两者间周旋。基本精神是在倡导保障隐私前提下，合规利用数据。不难看出为促进数据有效利用，以欧洲和中国为代表的监管主体都在为数据确权做出相应努力，从而使得数据在合规前提下自由流转，最终使得数据要素转变为经济要素，得以促进数字经济的发展。

技术增益：隐私计算技术蓬勃发展，为数据合规提供技术支持

原本为了保护用户隐私的监管措施，在世界范围内不断延伸落地、在不同领域掀起了数字经济变革。从结果来看，不仅没有阻碍数据流通，反而首先为数据确权、消费者权益保护、企业数据利用边界等诸多领域做出了应用的界定，由此促进数据合法合规利用，为数字经济规范化发展铺垫基础。

而早在政策、立法等动作之前，早有业界案例回响着数据滥用、隐私侵犯等问题。Netflix 在 2010 年的算法大赛可以看作是早期大企业在隐私问题上犯错的一个浓缩案例。Netflix 虽在技术上使用传统手段删去用户个人信息，但随着数字深入社会生活底层，多维数据可交叉验证成为新常态，旧有技术失去效力。

案例

Netlix 数据泄露事件

2010 年，Netflix（网飞）为了得到更好的影视剧推荐算法，举办了第二届“Netflix Prize”。Netflix 计划向有能力提升将算法精度提升 10% 的选手授予 100 万美元。

为了喂养算法，Netflix 主动向参赛者释放了 1 亿条信息，主要是用户电影观看记录、偏好类型及评分。数据中的用户个人身份信息已被 Netflix 提前删除，理论上无法定位到具体个人。

赛事最后吸引了超过 5 万名研究者参与，在机器学习研究领域中引发巨大反响。

然而这些数据在释出后遭到 UT-Austin（得克萨斯大学奥斯汀分校）两位研究者攻破，研究者利用 IMDB 数据库联合对比分析，还原了部分用户真实身份。随后 Netflix 因隐私问题引起了美国商务部注意及被提起诉讼，不久赛事宣告终结[5]。

类似的，以推荐算法为部分核心底层技术的互联网内容提供商都面临同样的境地。传统的隐私保护方案不再持续有效，亟待业界的更多技术进展弥补缺漏。而随着时间发展，部分国内外互联网大厂在 2C 场景应用差分隐私技术做出了成熟的实践案例，差分隐私技术核心在于本地对

[5] Taylor Buley. *Netflix Settles Privacy Lawsuit, Cancels Prize Sequel.* Forbes. https://www.forbes.com/sites/firewall/2010/03/12/netflix-settles-privacy-suit-cancels-netflix-prize-two-sequel/?sh=56c4b22a951e

技术增益：隐私计算技术蓬勃发展，为数据合规提供技术支持

用户个人信息数据添加随机“噪音”，随后上传至云端完成大规模统计等操作。这一技术使得原始个人信息数据不离本地，出库后的数据处于无法被还原、无法定位到个人的状态。

厂商	应用	功能
APPLE	输入法、应用耗电量检测	获取词语联想、app 耗电量情况
GOOGLE	谷歌地图	搜集地图的用户数量，计算出相应区域拥挤程度
小米	MIUI 手机系统地图应用	模糊定位，应用仅能获得用户大致位置

表 | 已投入成熟运用的差分隐私科技公司使用案例（来源：CB Insights 中国）

差分隐私科技公司使用案例 1： APPLE

响应用户忧虑与需求，2016 年前后苹果公司推出了“差分隐私”技术，意图在保护用户私人隐私前提下搜集数据，开拓数据获取渠道、喂养和迭代推荐算法，为用户提供更为精准的服务。苹果利用差分隐私技术搜集匿名用户信息，提供词汇联想、表情推荐、耗电量应用检测等服务[6]。

差分隐私科技公司使用案例 2： GOOGLE

最早在 2014 年前后便将其差分隐私技术应用于旗下应用：在谷歌浏览器中、使用差分隐私技术，谷歌搜集用户脱敏后的信息用于提升产品。在地图中，谷歌利用差分隐私技术汇集脱敏后的数据，勾勒交通流量。在 2019 年，谷歌宣布将旗下差分隐私技术库开源，为开发人员提供技术及交互界面。在新冠肆虐的 2020 年，谷歌在地图中搜集了脱敏之后的数据，掌握区域的拥挤程度，并提供报告，帮助相关公共健康部门采取相应措施、防控疫情[7]。

[6] Differential Privacy Team. *Learning with Privacy at Scale—Apple Machine Learning Research.* APPLE. https://machinelearning.apple.com/research/learning-with-privacy-at-scale
[7] Lily Hay Newman. *Google Wants to Help Tech Companies Know Less About You.* WIRED. https://www.wired.com/story/google-differential-privacy-open-source/

市场回响：隐私计算赛道投融资势头强劲

数据隐私作为一项基本的数据价值，在实际社会实践中往往体现为一个动态的认知过程，并且受社会文化、经济发展情况等不同维度因素所影响。随着中国监管加强，尤其在 2021 年随着《数据安全法》、《个人信息保护法》两部法律出台，数据流通和使用面临了更严格、更明确的合规要求。

以此为背景，隐私计算赛道在近年来掀起了投融资高潮，投融资趋势与近年来用户端的隐私意识崛起、政策端的监管加强有着高度相关性。目前，中国专注于隐私计算技术方案的公司融资阶段多集中在 A-B 轮，企业尚处成长性较大的早期阶段。

公司	融资时间	融资轮次	融资金额（元）	投资机构
洞见科技	2021-12-30	战略投资	数千万	中国电科、元起资本
融数智联	2021-12-15	A 轮	未披露	英诺天使基金、AC加速器、泰有投资、启迪之星
华控清交	2021-10-12	B 轮	5 亿	联想创投、中关村科学城、华兴资本
数牍科技	2021-09-27	A 轮	超 3 亿	GGV纪源资本、上海人工智能产业基金、深创投、红杉中国等
同态科技	2021-09-23	Pre-A 轮	数千万	东方富海、中南资本
锘崴科技	2021-08-09	B 轮	1 亿	东翰派富、致远互联、海南然格、黎刚资本、启明创投等
翼方健数	2021-07-29	B+ 轮	超 3 亿	未披露
冲量在线	2021-07-19	Pre-A 轮	数千万	元禾原点、IDG资本
富数科技	2021-07-15	C 轮	数亿	中网投、同创伟业

表 | 2021H2 中国隐私计算行业部分投融资事件（来源：CB Insights 中国）

Chapter 2

利器：

隐私计算三类技术路线，六个技术子项

- 隐私计算技术综述
- 隐私计算技术子项
  - 安全多方计算（MPC）
  - 同态加密（HE）
  - 差分隐私（DP）
  - 零知识证明（ZK）
  - 联邦学习（FL）
  - 可信任执行环境（TEE）

隐私计算技术综述

在技术基本定义层面，需要指出的是“隐私计算”并不单指一项具体的可以落实的技术项目，而是以实现数据隐私和数据合规目的为驱动的多个路线的一箩筐技术项。

在中文语境下，保护隐私的相关技术合集最常被称为“隐私计算“。在英文语境中常见有两种称谓：例如英国皇家学会研究称之为 Privacy Enhancing Technologies（PET，隐私增强科技）[8]，而在联合国大数据工作组的研究中则被称为 Privacy-Preserving Computation Techniques（PPT，隐私保护计算技术）[9]。

在这些不同的研究中，命名的语义上各有侧重，所涵盖的技术子项则不尽相同。在主流英文产业研究中，且除了咨询研报面向产业、以数据价值为导向，常见的 PET 和 PPT 公开研究许多由公共机构推动、以数据治理为导向，侧重于宣扬技术宏观社会价值，这一点与中国或偏向技术或以商业为导向的研究有所区别。

根据目前中国业界普遍认可的技术范畴取概念共识，隐私计算指的是包含了安全多方计算、同态加密、差分隐私、零知识证明、联邦学习以及可执行环境等主流技术子项的相关技术合集及产品方案。

本报告将上述技术分为三大路径：以安全多方计算为代表的密码学路径、以可信任执行环境为代表的硬件路径和以联邦学习为代表的人工智能路径。在法律法规、产业落地多维趋势之前，三大路径的隐私计算研究应用早已开启，并且按照各自技术路径呈现了各自发展脉络：

[8] Royal Society (Great Britain). (2019). *Protecting privacy in practice: The current use, development and limits of privacy enhancing technologies in data analysis.*
[9] The Privacy Preserving Techniques Task Team (PPTTT). (2018). *UN Handbook on Privacy-Preserving Computation Techniques.*

隐私计算技术综述

- **安全多方计算（MPC）：**早在 1986 年，著名计算机科学家、图灵奖得主姚期智教授提出了两方之间的安全计算设想方案，以会议论文《How to Generate and Exchange Secrets》为标志开启了安全多方计算（Secure Multi-party Computation）的研究路径[10]。

- **可信执行环境（TEE）：**在 2003 年，由 Ben Pfaff 等人讨论了可信执行环境，并将其定义为“专用的封闭虚拟机，并与平台的其他部分相隔离。并通过硬件内存保护和储存加密保护，使其内容免于未授权方的探查和篡改。”在 2009 年则有移动终端行业论坛 OMTP（开放式移动终端平台组织）提出了“高级信任环境”的设想[11]。

- **联邦学习（FL）：**在 2016 年，以 Brendan McMahan 为代表的一组谷歌研究者提出了一种深度网络的联邦学习，以解决大数据训练过程中的隐私难题。该方案通过将数据训练工作从中心节点下放至分布式本地手机设备，利用分散的本地化算力本地提取模型，其次二次汇集模型、中心化训练这些模型从而完成训练流程，由此开启了联邦学习研究与应用[12]。

在早期，不论是中国的研究亦或是欧美以政府、研究机构主导的相关研究都将“隐私计算”放置于数据安全、数据隐私领域全链路主题下，从维护民众和用户的隐私权利出发，使其免于商业乃至其他利益侵害，相关技术合集“隐私计算”往往是一个泛化的概念，并不被视为整一、独立且严格定义的技术范畴。

[10] Domingo-Ferrer, J., & Blanco-Justicia, A. (2020). Privacy-Preserving Technologies. In *The Ethics of Cybersecurity* (pp. 279-297). Springer, Cham.
[11] Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: what it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 57-64). IEEE.
[12] 刘俊旭, & 孟小峰. (2020). 机器学习的隐私保护研究综述. *计算机研究与发展*, 57(2), 346.

隐私计算技术综述

针对上述研究和业界现状，2016 年中国科学院信息工程研究所李凤华等人发表了《隐私计算研究范畴及发展趋势》，初步定义了严格的“隐私计算”范畴[13]。随后在 2019 年发表了《隐私计算——概念、计算框架及其未来发展趋势》的论文，明确了隐私计算的理论体系，从而将这一概念正式落地[14]。今日业界所讨论的“隐私计算”概念和技术基本与文中的研究相印证，系列论文和讨论内容可以看作是隐私计算范畴凝练的开启与总结。

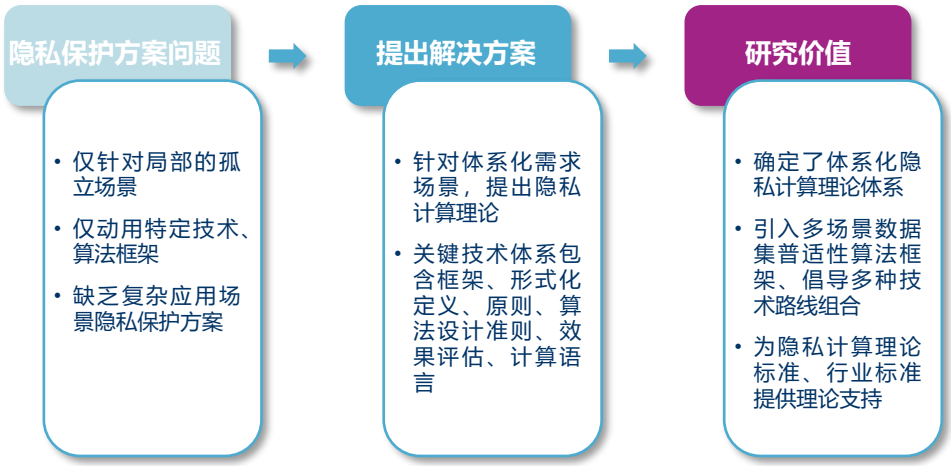

图 | 2019 年李凤华等人对隐私计算的总结性研究（来源：CB Insights 中国整理）

同样需要指出的是，尽管“隐私计算”是新的技术概念和范畴，在商业端呈现了所有新兴技术产业化落地的特征，但隐私计算所涵括的多数技术子项在纯研究与方案设想方面已经发展成熟（譬如安全多方计算可追溯至上世纪 70、80 年代）。与技术导向性较强的商业应用类似，隐私计算业界基本是将成熟的技术研究产品化落地在不同场景进行调试并在终端探索更好的产品。因此行业总体呈现出研究先行、商业落地则在工程化、产品化上发力的特点。

[13] 李凤华, 李晖, 贾焰, 俞能海, & 翁健. (2016). 隐私计算研究范畴及发展趋势. *通信学报*, 37(4), 1-11.
[14] 李凤华, 李晖, 牛犇 & 陈金俊. (2019). 隐私计算——概念、计算框架及其未来发展趋势. *Engineering*(06).

隐私计算技术子项——安全多方计算（MPC）

技术简述：安全多方计算（Secure Multi-party Computation, MPC）是一种密码学领域的隐私保护分布式计算技术。安全多方计算能够使多方在互相不知晓对方内容的情况下，参与协同计算，最终产生有价值的分析内容。

安全多方计算适用于有多方联合计算需求、同时不想暴露己方信息的情境，尤其在法律禁止多方数据共享的某些情境下，具有较强应用意义。安全多方计算过程并不需要可信第三方的参与，因此理论上安全等级较高。

技术局限：由于安全多方计算采用的是密码学路径，相比于明文数据计算消耗更大算力。同时，分布式计算架构致使其具有延迟，因此总耗时也延长。此外安全多方计算还面临密钥可能泄露带来的安全、隐私挑战。

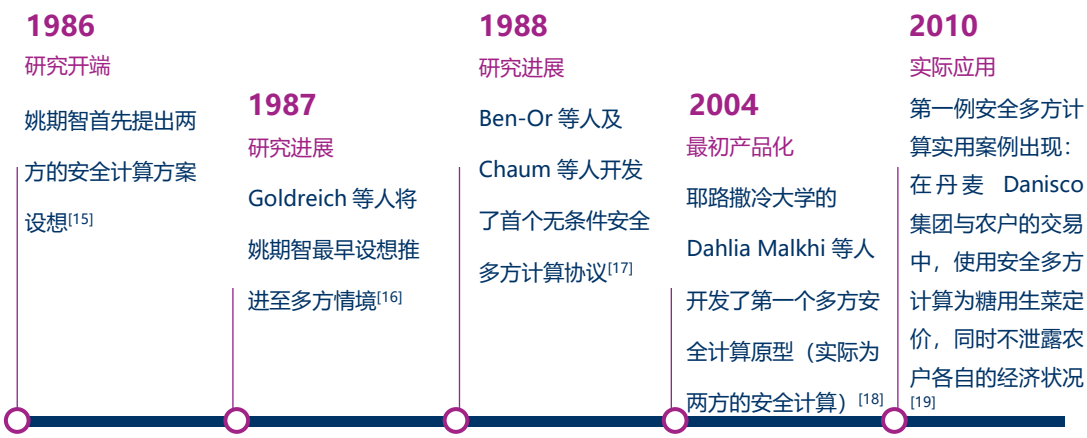

图 | 安全多方计算的研究、产品化历程（来源：CB Insights 中国）

[15][16][17] Domingo-Ferrer, J., & Blanco-Justicia, A. (2020). Privacy-Preserving Technologies. In *The Ethics of Cybersecurity* (pp. 279-297). Springer, Cham.
[18] Malkhi, D., Nisan, N., Pinkas, B., & Sella, Y. (2004, August). Fairplay-Secure Two-Party Computation System. In *USENIX Security Symposium* (Vol. 4, p. 9).
[19] Damgard, I., & Toft, T. (2008). Trading sugar beet quotas: secure multiparty computation in practice. *Ercim News*, (73), 32-33.

隐私计算技术子项——同态加密（HE）

技术简述：同态加密（Homomorphic Encryption，HE）指的是能够直接使用密文进行特定运算的加密技术。在同态加密计算过程中，无需密钥即可实现操作，而结果仍需密钥解密从而变为明文，在解密后，得到与明文计算相同的结果。

同态加密可直接对密文进行分析、检索。因此在达成保护隐私的前提下，还能实现某些数据操作。同态加密实现了数据使用过程（Data in use）中的加密，适用于部分诚信和恶意环境中，以保护数据安全与隐私。目前适用场景有医疗数据加密、顾客数据分析、多个机构间客户的交叉分析等。

技术局限：技术仍旧处于早期成熟阶段。相比于明文计算，同态加密后的计算流程算力消耗巨大同时数据吞吐量较低。此外，由于同态加密后的数据体积增大、将会挤占网络带宽。因此，诸如全同态加密在运行速度随着数据量增多、计算耗时急剧增多等问题仍有待研究持续推进。

图 | 同态加密的研究、产品化历程（来源：CB Insights 中国）

[20] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11), 169-180.
[21] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. *In Proceedings of the forty-first annual ACM symposium on Theory of computing* (pp. 169-178).

隐私计算技术子项——差分隐私（DP）

技术简述：差分隐私（Differential Privacy，DP）是通过添加额外的随机数据“噪音”使真实信息淹没于其中，从而保护隐私的一种技术手段。在增加“噪音”的同时，差分隐私还允许汇合数据时进行精确计算。其优势在于，即使有恶意用户使用结果数据集反推原始数据，由于数据集中存在数据“噪音”，无法辨识数据真假，因此难以还原原始数据。与密码学其他相关协议相比，其优点在于无须加密、解密过程中的巨大算力消耗，可处理相对大型的数据量，效率较高。

目前差分隐私技术相对成熟，应用较为广泛，例如 APPLE、GOOGLE、小米等案例。在公共领域，美国在 2020 年人口普查过程中就使用了差分隐私技术，在保障民众隐私的前提下释放更多细微颗粒度的人口信息，使得更多维度、更有深度的信息得到广泛传播进而服务于研究领域、公共政策以及知识传播。

技术局限：差分隐私点在于因为在原始信息中添加了不少的噪声，因此进行数据的汇总处理时，不可避免导致数据的精确度产生偏差。

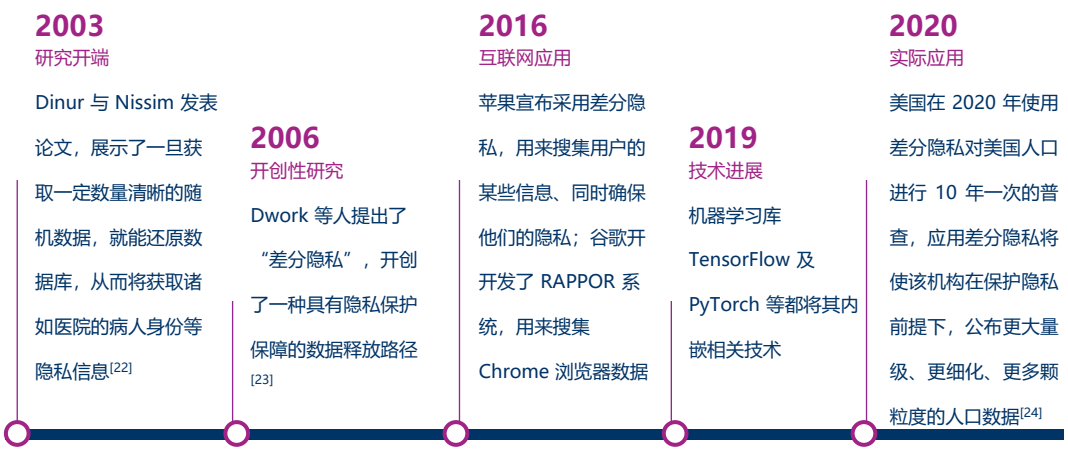

图 | 差分隐私的研究、产品化历程（来源：CB Insights 中国）

[22] Dinur, I., & Nissim, K. (2003, June). Revealing information while preserving privacy. *In Proceedings of the twenty-second ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems* (pp. 202-210).
[23] Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006, March). Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference* (pp. 265-284). Springer, Berlin, Heidelberg.
[24] Garfinkel, S. L., Abowd, J. M., & Powazek, S. (2018, January). Issues encountered deploying differential privacy. In *Proceedings of the 2018 Workshop on Privacy in the Electronic Society* (pp. 133-137).

隐私计算技术子项——零知识证明（ZK）

技术简述：零知识证明（Zero Knowledge Proofs, ZK）是一种可让一方（需求方）面对另一方（验证方）时，证明其陈述为真、同时无需暴露己方信息的密码学技术。

零知识证明适用于有向其他人验证的需求，同时又不希望暴露信息的场景。例如，一个典型的适用场景为证明论断“张某是超过 18 岁的成年人”为真，在某些场景下，张某同时需要证明成年，同时又有顾虑不愿透露真实年龄。

在现实世界中，零知识证明已经在区块链的诸多场景下落地，典型场景有证明交易过程中己方交易的合规性。加密货币 ZeroCash（大零币）就使用了零知识证明技术避免交易的支付方、收款方、数量等信息泄露，同时证明交易相关信息的正确性。

技术局限：目前零知识证明仍是一种较为早期的技术，有待更多场景和产品落地。同时技术标准欠缺，有待行业标准化的持续发展。

1985
研究开端
Shafi Goldwasser(MIT) 等人在 1985 年首次提出零知识证明的概念，用以证明论述为真同时不泄露其他信息[25]

1986
首个广泛认可的研究
1986 年，Goldreich 等人探讨了使用任意承诺方案构建零知识证明系统，成为首个相对广泛场景可应用的零知识证明系统[26]

1999
研究进展
Feige 等人基于“证人不可区分”理念完成了零知识证明的重要技术[27]

图 | 零知识证明研究历程（来源：CB Insights 中国）

[25] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1), 186-208.
[26] O. Goldreih, S. Miali and A. Wigderson. Proofs that Yield Nothing but their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. *Journal of the ACM*, Vol. 38, No. 1, pages 691{729, 1991. Preliminary version in 27th FOCS, 1986.
[27] U. Feige, D. Lapidot, and A. Shamir. Multiple Non-Interative Zero-Knowledge Proofs Under General Assumptions. *SIAM Journal on Computing*, Vol. 29 (1), pages 1{28, 1999.

隐私计算技术子项——联邦学习（FL）

技术简述：联邦学习（Federated Learning，FL）是一种采用分布式结构的机器学习技术。传统的机器学习过程主要使用中心化方式进行，而联邦学习则首先利用分布式数据进行本地化模型训练，其次将所得到的模型结果汇总至中心节点，进行二次训练后得到最终的训练模型。

在这个过程中，中心节点无法看到原始数据，而只能得到模型结果，因此有效地保证了过程的隐私。在联邦学习过程中，由于中心节点得到的只是模型结果而非原始数据，因此适用于多种场景需求。例如，由于法律限制而不能共享某些数据库的情况下，联邦学习可以使得需求方避免获取原始数据、而同时得到需求结果。

技术局限：与中心化的机器学习路径相比，联邦学习由于多了额外模型提取过程，因此最终训练的模型结果在精度上往往不敌前者。同时，由于联邦学习本质上仍是一种机器学习，而隐私保护则是一种功能，因此还需要与其他隐私计算技术相结合，才能充分保障隐私。

2016
研究开端

H.Brendan McMahan 等人提出联邦学习，应用于谷歌输入法，实现输入法的候选词预测[28]

2016 至今
研究进展

2016 年，Jakub Konecny 等人进一步提出优化算法用以处理数据分布的问题。随后涌现了一大批提升训练效率、提升联邦学习公平性等技术面提升研究[29]

近年
开源框架涌现

谷歌提出的 TensorFlow Federated 框架，OpenMind 提出的 Pysyft 框架，微众银行提出的 FATE 框架，百度提出的 PaddleFL 框架

图 | 联邦学习研究与产业化历程（来源：CB Insights 中国）

[28] 梁天恺, 曾碧, & 陈光. (2021). 联邦学习综述: 概念, 技术, 应用与挑战. *计算机应用*.
[29] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.

隐私计算技术子项——可信任执行环境（TEE）

技术定义：可信任执行环境（Trusted Execution Environment, TEE）指的是为保障数据和代码相对保密和完整，设置的一种独立于系统其他部分的处理执行环境，该环境包含了记忆存储设备和计算能力，并且能够抵御软件层面的外界攻击以及物理层面对系统主存储器的攻击。

与密码学路径的相关技术不同，可信任执行环境主要由特殊的硬件提供外在的安全环境。在实际运行时，数据以明文形式进行，因此在运算速度上具有优势。

产品案例：目前，主流的支持可信执行环境的平台有 ARM 发布的 TrustZone 和 Intel 发布的 SGX。TrustZone 区分了安全与非安全两个分界，例如密码处理、指纹识别等保密操作需要在安全区域运行，其余则在非安全区执行。而 Intel SGX 主要实现了不同程序隔离运行，将合法软件的安全操作封装于飞地（Enclave）中，而免于恶意软件的攻击。

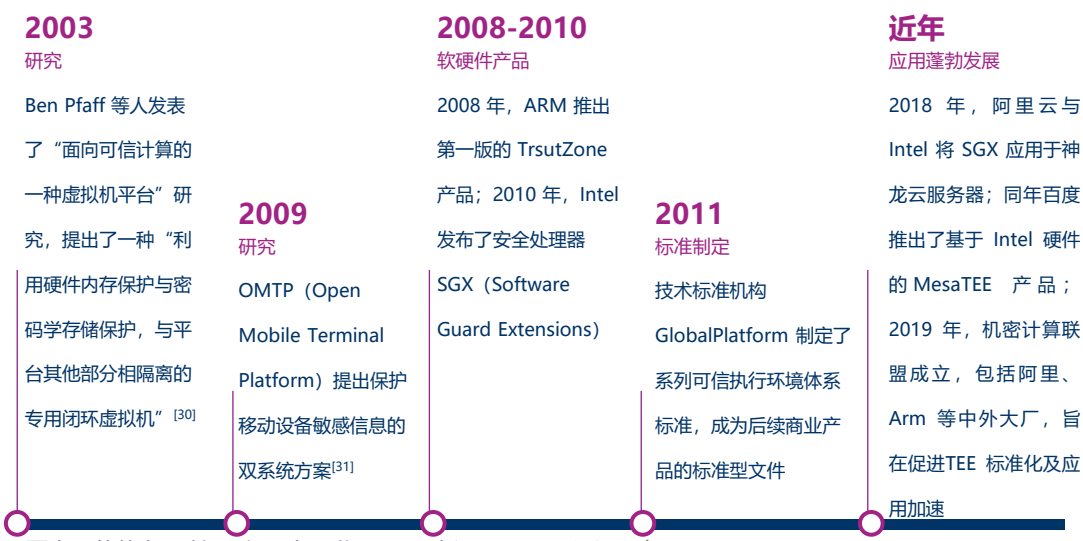

图 | 可信执行环境研究、产品化历程（来源：CB Insights 中国）

[30] Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., & Boneh, D. (2003, October). Terra: A virtual machine-based platform for trusted computing. In Proceedings of the nineteenth ACM symposium on Operating systems principles (pp. 193-206).
[31] OMTP. (2009). OMTP advanced trusted environment OMTP TR1.

隐私计算技术子项——可信任执行环境（TEE）

此外，还有部分新的基于 RISC-V 的开源处理方案，仍处于研发和应用的早期阶段。目前，基于 ARM 和 Intel 的硬件产品，国内陆续有百度的 MesaTEE、华为 iTrustee 等产品方案提供服务。在场景上，主要落地在云服务与手机应用。

技术局限：在可信任执行环境下，数据的处理速度通常与明文处理速度相差不大。根据研究，与明文处理速度相较，当数据量处于 100MB 水平的时候，可信任执行环境下的数据处理速度可能会下降至多 20%。然而一旦数据量增多，当数据处于 GB 级别的情况下，速度可能会折损 5-7 倍（同时表现仍大幅领先安全多方计算和全同态加密）。

此外，现有成熟的可信执行环境方案底层硬件主要采用了 Intel 和 ARM 的产品。使用相关方案和产品，意味着将数据泄露、数据确权等疑虑托付至这些厂家，一旦涉及到敏感的数据、以及数据主权等问题，相应会带来一定顾虑。

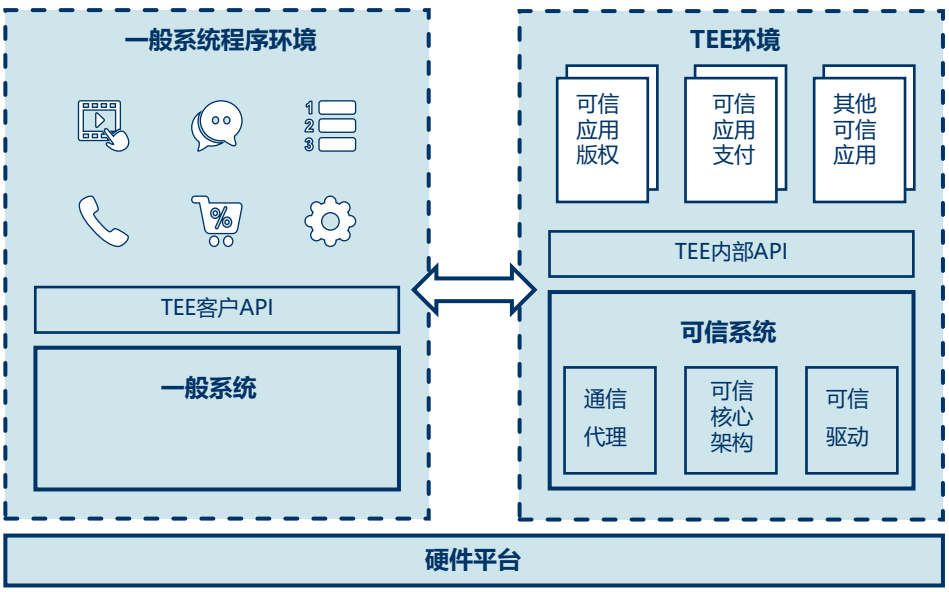

图 | ARM TrustZone 产品结构示意图（来源：CB Insights 中国）

	安全多方计算（MPC）	同态加密（HE）	差分隐私（DP）	零知识证明（ZK）	联邦学习（FL）	可信执行环境（TEE）
实现路径	■ 数据系统与结构化	■ 数据遮挡	■ 数据替换	■ 数据系统与结构化	■ 数据模型	■ 数据隔离
保护数据阶段	■ 使用状态数据 (Data in Use)	■ 存储状态数据 (Data at Rest) ■ 使用状态数据 (Data in Use)	■ 使用状态数据 (Data in Use)	■ 使用状态数据 (Data in Use)	■ 使用状态数据 (Data in Use)	■ 存储状态数据 (Data at Rest) ■ 使用状态数据 (Data in Use)
优势特点	■ 理论上无需第三方参与 ■ 直接得到结果和模型	■ 无数据信息损耗	■ 可根据需求添加“噪声”的量级，适用于多场景	■ 达成特定目的且仅提供最低限度信息	■ 原始数据不出库 ■ 分布式架构降低总算力成本	■ 数据信息无损耗 ■ 域内无算法限制 ■ 现有成熟方案多
技术局限	■ 所需算力较大、耗时长 ■ 秘钥泄露存在可能	■ 算力消耗大 ■ 随着数据增多，运算速度减缓显著，挤占网络带宽	■ 添加“噪声”后，数据精准度下降	■ 理论上安全性未被完全证实和广泛接受 ■ 某些类型的计算过程效率较低 ■ 标准化程度不高	■ 数据模型质量参差不齐 ■ 通信复杂度较高 ■ 隐私保护无密码学验证	■ 可能面临侧信道攻击
成熟度	■ 产品化落地	■ 已产品化、仍处于早期	■ 产品化落地	■ 产品化落地、方案不多	■ 产品化落地	■ 产品化落地、方案较多

Chapter 3

索骥：

四类玩家，各据禀赋、共拓市场

- 产业链路：数据利用涉及三方，合规监管伴随始终
- 隐私计算行业图景：四类玩家，各据禀赋、共拓市场
- 产业案例：政务、金融、医疗三大场景

产业链路：数据利用涉及三方，合规监管伴随始终

在宏观层面上，根据数据使用流转序列，隐私计算行业在数据链上主要包含了四大主体：数据来源方、数据需求方、隐私计算方案提供方，以及业务之上负责对数据全流程实施监督的监管机构。

数据来源方：一般为电信运营商、征信平台、掌握公共数据的相关政府部门、各地大数据交易中心等机构，该类机构提供原始的通信、政务等不同类型数据；

数据需求方：分为金融、政务、医疗等三大行业的不同机构，终端应用场景包含信用评估、风控、数据合规共享等。随着合规、隐私保护方面需求渐盛，行业与场景正在逐渐拓展中，例如近期涌现的新需求方包含了车企等新类别；

数据服务方：隐私计算企业在全链路中充当了技术供给、数据赋能的角色，使得数据可以合规交换利用；

行业监管机构：主要包含中国各地大数据局、发改委等机构，在合规的层面上对产业各个主体提出要求，监督数据隐私、数据安全落实情况，最终保障敏感信息不会威胁到国家、重要机构、个人的安全。

图 | 隐私计算行业数据链路示意图（来源：CB Insights 中国）

隐私计算行业图景：四类玩家，各据禀赋、共拓市场

深入行业图景，随着近年来技术增益与商业落地场景逐步丰满，涌现了一大批包含隐私计算能力并有能力实践产品落地流程的企业。其中，他们或是在原有厂商业务之中拓展新的技术手段和生成新的技术产品，或是利用新技术延续既有业务模块、以满足合规需求，或是完全以成熟的隐私计算技术为核心底座从事商业运营的隐私计算商家。

在中国隐私计算行业现有玩家图景中，玩家依据各自性质、沿革、战略打法、资源禀赋的多个维度，分为四类：“大厂生态型”、“隐私计算专攻型”、“行业赋能型”、“人工智能、区块链技术型”。各类玩家在积极推高技术渗透率与拓展应用边界的行业发展趋势中，一同构成中国现有隐私计算行业厂商图景：

中国隐私计算厂商图景

图 | 中国隐私计算厂商图景（来源：CB Insights 中国）

隐私计算行业图景：四类玩家，各据禀赋、共拓市场

大厂生态型：

概述：包含以腾讯、百度、蚂蚁集团为代表的互联网大厂系玩家。该类互联网科技公司汇集了海量的 C 端用户数据，天然是数据富集地，隐私计算直接服务于数据使用过程中的隐私保护工作，能充分赋能大厂生态中的数据利用，是其技术能力矩阵中坚实的一环。

特征：在规模上大厂隐私计算团队往往与专攻型团队相当，在商业利用链条中主要立足于集团数据生态、服务内部数据利用为主。同时由于生态系统属性不同，各家互联网科技公司生态下的隐私计算能力和资源打通相较之下主动性不足。

行业赋能型：

概述：主要指的是应用隐私计算技术赋能主营业务的玩家，典型代表包括金融科技公司的平安科技、微众银行。从隐私计算赛道的角度，这些公司主营业务早已成熟，在专精领域商业拼图上已经取得显著地位。随着业务的发展及合规需求，这些公司从技术能力版图和业务需求出发，打造团队钻研隐私计算技术，使得技术服务于成熟的业务板块。

特征：从隐私计算技术与产品落地能力角度出发，该类公司技术应用领域主要集中在原有行业，因资源优势战略上也较为聚焦特定行业。

隐私计算行业图景：四类玩家，各据禀赋、共拓市场

隐私计算专攻型：

概述：该类公司主要指的是随着隐私计算行业热潮而生的一大批专注于隐私计算技术与产品的公司，典型企业有华控清交、数牍科技、洞见科技、锘崴科技等。这类公司位于行业竞合舞台的核心，创造了行业不断变动的现状。他们往往成立时间约在五年以内，尤其在 2019-2020 年间集中诞生。

特征：在资源禀赋上，该类公司核心团队往往是隐私计算领域科研领军人物、技术专家，或在密码学、人工智能领域研究具有突出贡献，或曾于国内外大厂隐私团队担任要职，以此为契机和创业起源开疆拓土。该类企业在技术上普遍倾向于打造“通用型”隐私计算技术，因此在隐私计算市场中未来商业形态的可塑性、可拼合程度较高。由于创立时间尚短、行业生态并未完全定型，这类企业在商业化图景上仍有待持续发展。

人工智能、区块链技术型：

概述：主要从事人工智能技术方案研发与区块链技术研发为主的公司。与主业务赋能型企业类似，该类企业主要将隐私计算能力拼合到整体技术模块，服务于企业战略。该类企业的鲜明特征在于立足于技术研发与供给，对外输出综合技术能力。

特征：该类企业优势在于以技术为核心驱动力，在既有的商业版图中已经有过多个成熟案例，对客户需求理解较深。隐私计算作为新近涌现的需求，在商业侧对该类企业而言并不陌生，且有相关案例及既有资源池可倚赖。

蚂蚁集团：提升医疗模型准确度，实现精准控费

蚂蚁集团是一家金融科技开放平台公司，旗下蚂蚁隐私计算智能服务平台“隐语”围绕算法、系统、应用展开，是具备高性能、可扩展性的工业级隐私保护学习平台。“隐语”可破解数据资产分布式存储和分属不同主体情境下的关键技术难题，确保数据安全、实现隐私保护的协同计算，达到多方机构间信息聚合和资源共享目的。

目前已应用于包括联合信用风控、联合反欺诈/反洗钱风控等金融场景，和对个人隐私高度敏感的医疗、政务等数字经济典型场景。据国家工业信息安全发展研究中心数据，蚂蚁集团拥有业内最多的隐私计算专利数量。

案例概述：“医疗诊断相关分组”（DRGs）是一种病例组合分类方案和医保支付方式，即根据年龄、疾病、资源消耗因素将患者分入若干诊断组进行管理的体系。基于诊疗数据预测，医保局最终给定分类实现精准控费。在此体系下，单家医院由于数据体量、疾病覆盖度不够，因此自有数据训练模型效果欠佳。采用多方安全计算及联邦学习技术方案，蚂蚁平台使用“隐语”依国家医疗保障局公布的 CHS-DRGs 分组规范，将多家医疗机构数据进行联合训练。在保护患者隐私前提下，增加样本数量、扩大数据规模，最终获得更为准确的 DRGs 分类模型，帮助医疗机构进行 DRGs 预测。

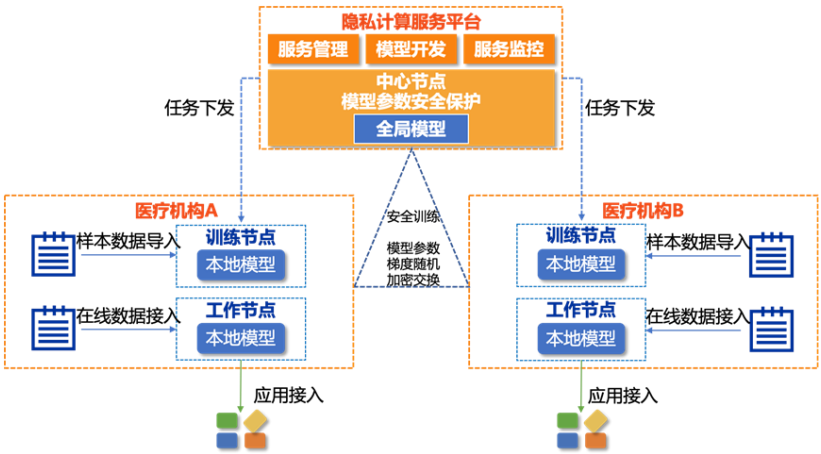

图 | 蚂蚁隐私计算服务平台在医保 DRGs 建模中应用总体框架（来源：蚂蚁集团）

蚂蚁集团：提升医疗模型准确度，实现精准控费

蚂蚁方案落地七个环节

初始化

医疗机构 A 和医疗机构 B 在本地进行隐私保护计算节点部署，并进行网络授权和调试，待初始化完成后即开始具体联合建模的项目的运营。

数据准备

医疗机构 A 和医疗机构 B 分别通过阿里云医疗大数据管理平台，选择各自的 DRGs 分组数据集的样本数据，加载到各自本地隐私保护计算节点上，在平台上进行对应样本的数据表结构注册并授权进入联合项目。

隐私求交

平台上选择双方注册授权表进行隐私求交指令操作，实现两方样本数据对齐，形成虚拟宽。

联合建模

针对虚拟宽表进行模型训练，包括数据预处理、特征工程、特征筛选、算法调优以及模型评估，待模型训练完成后产出模型评估报告由联合项目机构进行线下模型评审，待完成后即可进入模型服务部署阶段。

模型发布

机构针对提交的联合模型各自开发特征服务，以 API 形式对接本地隐私保护计算节点；而后在平台进行特征定义，并将模型与特征绑定后发布。

服务集成

服务集成在平台进行操作，主要针对已发布的模型进行出入参配置，以及调用服务流程编排，并进行服务链路验证保证。待上述步骤完成后即可进行服务部署，一般以 API 形式由服务需求方（比如金融机构的决策系统）进行调用。

服务监控

服务正常运行时，平台提供全链路服务监控用以监控联合模型服务的调用情况以及运行时模型稳定性的监控。

部署与效果：案例基于蚂蚁隐私计算框架“隐语”的多方安全计算及联邦学习技术，通过阿里云医疗大数据管理平台落地，采用七个环节使医疗机构实现了数据不出本地、数据隐私保护有所保障，同时扩大了模型训练数据规模，从而提升了本地 DRGs 模型分组预测的准确度。

大规模医院因数据多通常准确率较高，但较小规模医院的分组预测模型准确率则明显受制于数据量限制，难以与之相比。使用两家医院数据后，其模型预测准确率可有显著提升。具体到某分组预测准确率，采用方案后，显著提升的为出现频次较低的 DRGs 。如某个 DRGs 在某地区医院 A 比较少见，在另一地区医院 B 常见，两者结合后 A 医院的 DRGs 准确率可有显著提升。

以某医院为例，选定 DRGs 模型训练样本主题数据集，基于隐语服务作为隐私保护计算节点之一进行联合训练后的 DRGs 模型的分组预测准确率提升显著。

洞见科技：守卫政务数据安全，以自适应隐私计算引擎服务应用场景

洞见科技是中国最大的信用管理集团“中诚信”孵化、网信事业国家队“中国电科”投资的隐私计算技术服务商，致力于以隐私计算技术赋能数据价值的安全释放和数据智能的合规应用。公司的创始团队是中国大数据征信和智能风控行业的推动者和领军人物，核心成员来自中诚信、大型银行、保险公司以及人工智能企业，具备丰富的行业知识和服务经验。

洞见科技于 2020 年初推出国内首个面向计算场景的隐私安全计算产品——洞见数智联邦平台（InsightOne），围绕数据资源融合和业务场景应用构建安全可信的数据智能联邦，目前已在政务、金融等领域落地了大量隐私计算合作案例，应用场景覆盖联合风控、联合营销、资产扫描、精算定价、存客激活、数据要素流通、银企融资对接、债券指数编制等。

融合引擎架构产品体系，根据场景智慧调度高性能隐私计算能力

多维海量数据为各行各业带来了革命性的智慧变革，赋能算法为终端应用提供源源不断的活水源头，由此在政务、银行、保险、智慧城市等领域不断产生新应用，全面提升数字经济智能程度。对隐私计算行业而言，海量数据与多维场景同时也意味着数据处理工程面临巨大挑战。

图 | 洞见隐私计算产品——数智联邦平台 InsightOne（来源：洞见科技）

洞见科技：守卫政务数据安全，以自适应隐私计算引擎服务应用场景

对此洞见科技隐私安全计算平台 InsightOne 采用面向终端场景的融合式架构，以“左加数据、右加场景”的模式，链接数据需求方与供给方，在数据源头与应用场景之间架起“自适应桥梁”，使得隐私计算能力依据终端需求特点，自动调用最匹配的技术引擎。

在隐私安全计算方面，洞见数智联邦平台（InsightOne）以安全多方计算和可信联邦学习为主计算引擎，辅以可信执行环境、差分隐私、零知识证明等多技术项为不同场景提供可定义的计算能力，具有高安全性、高兼容性、高连接性、高灵活性、高专业性等特点，实现“数据可用不可见”。同时，通过隐私计算的智能合约化和算法容器化等技术，构建分布式信任机制和互联互通能力，实现“计算可信可链接”。

在高性能计算方面，基于 InsightOne 平台，洞见科技进一步研发了融合计算、网络、存储、FPGA 加速卡为一体的 InsightBox 隐私计算软硬件一体机产品，可突破传输瓶颈，提供十亿级别数据量的计算能力，具有全栈可信、强劲综合性能、高兼容设计、海量数据存储、国产信创等特点，满足政府与企业在数据协同、共享、交换等场景的高性能计算需求。

案例：保障数据合规应用、挖掘数据要素红利，洞见科技助力国内首个省级政务数据隐私计算平台建设

案例背景：国内各地数据平台、数据交易中心处于蓬勃建设热潮中。随着政策法规出台，隐私保护和数据合规要求日益明晰，政务数据开放面临着数据隐私保护和数据开放流通的两难局面。2021 年，山东省计划建立全省一体化的公共数据开放平台以实现数据综合集约化管理。为此，洞见科技联合智慧齐鲁公司，以“数据可用不可见、计算可信可链接”的隐私保护计算技术，为山东省大数据局建设了国内首个省级政务数据隐私计算平台。

洞见科技：守卫政务数据安全，以自适应隐私计算引擎服务应用场景

案例详述：该省级政务数据隐私计算平台基于洞见数智联邦平台（InsightOne）成熟框架开发，技术架构上由数据平台层、数据计算层、数据服务层和运营支撑层组成，在原始数据不出域前提下通过联合计算、联合建模等功能安全得出计算结果，实现多机构间的数据协同计算与数据资源合规市场化、安全应用化、价值最大化，并通过“图形化”交互实现联邦学习建模，可视易用。全流程通过区块链可信网关记录计算过程与价值贡献，实现可追溯、可计量、不可篡改。

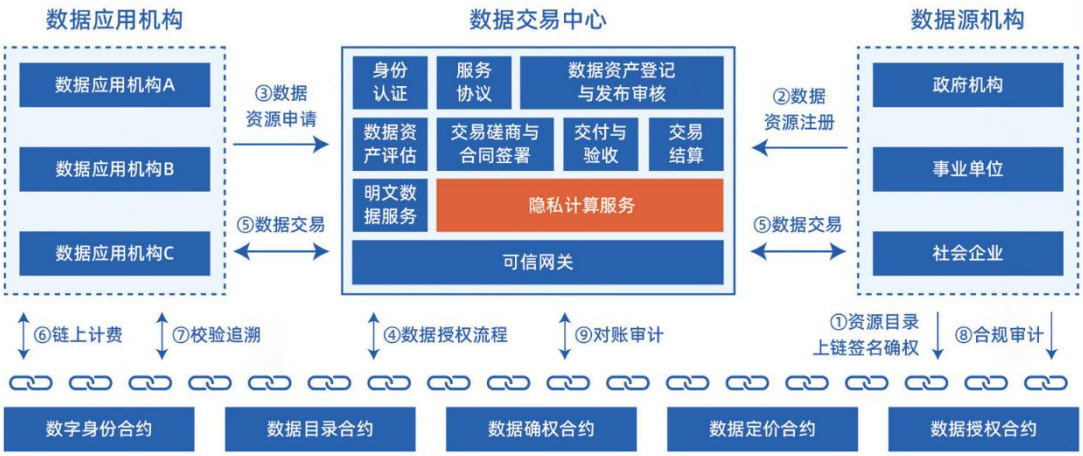

图 | 洞见科技“隐私计算+政务数据要素流通”解决方案（来源：洞见科技）

案例成效：方案为政府内、外部数据需求方提供安全可信的政务数据隐私计算服务，推动政府数据智能生态体系建设，实现数据价值“重组式”创新。一、实现跨域数据开放融合业务应用全生命周期安全保障，并实现外部公共数据分布式访问和对异构应用访问的适应性；二、构建良性闭环的数据价值链生态。突破跨域数据壁垒，打通跨域数据的应用价值链，使得数据基于业务应用需要在各个企业之间安全地共享和流通；三、通过构建“政务数据隐私计算平台”底座，加快推进数据在数字金融、智慧城市等领域的场景应用和生态建设，并在保护数据隐私安全的前提下，进一步提高公共数据融合和流通服务质量及效率，形成社会效益与经济效益双发展。

数牍科技：助力金融、政务等场景，打造数据要素安全流通基础设施

成立于 2019 年这一国内隐私计算行业初始阶段，数牍科技强调隐私计算领域的“系统性综合工程视角”，通过打造面向数据要素流通的合规方案和产品，包括隐私计算平台、数据治理工具等，以应对技术侧逐渐趋同的行业现状。数牍重视产品打磨修炼，采用多方安全计算、联邦学习与分布式系统技术项服务于数据融合、联合建模及数据应用。数牍现有合作客户包括政府机构、央企、金融保险、互联网公司，覆盖政务、金融、营销、风控、医疗等场景。典型客户有三大运营商、银联、工商银行、北京银行及各地数据交易所。

图 | 以数据生命周期为视角、多技术融合——数牍科技隐私计算平台 Tusita（来源：数牍科技）

案例 1：为数据要素流通基础设施建设打好技术底座，优化市场接入体验

数牍科技发挥隐私工程能力优势，帮助多个大规模数据安全协作工程建设隐私技术底座，并通过“数商”身份，推动数据要素流通与交易的标准化。目前，数牍科技已成为北京、上海、深圳、重庆、合肥等多地数据交易所首批数商及交易平台建设方。

数牍科技：助力金融、政务等场景，打造数据要素安全流通基础设施

在符合监管要求的前提下，一方面，数牍科技协助交易所完善和优化交易机制（包括数据合规、数据产品上架和定价建议，以及数据承销，数据资产化等服务），另一方面，面向数据应用主体，通过构建包括数据产品、模型产品等在内的多层次产品体系（提供包括数据交易公证，数据贡献度评估等配套服务，提供灵活、安全的隐私计算可视化建模能力），优化市场接入体验，并积极引入、撮合更多的数据开放主体，从而更好的满足数据应用主体需求。

案例 2：广开数源，破解普惠信贷风控难题

长期以来，小微企业在经济民生中占据了重要地位。然而小微企业往往或尚处初创阶段，或受制于营收、贷款等既有金融记录匮乏困扰，对银行而言，相关金融服务的风险控制难度大导致服务能力受限，因此小微企业获取到的金融扶持较少，许多尚处于萌芽阶段的未来成功企业难以获取足够的金融支持。

对此，数牍科技在 2021 年与某国有银行及数据伙伴共同完成了“基于隐私计算的普惠信贷风控服务”，融合多方数据源、提升风控评级精准度，降低不良借贷风险。数牍科技应用了联邦学习等隐私计算技术，在不收集、不存储原始数据前提下，实现银行与数据合作伙伴双向信息隐蔽下的用户特征探查和模型特征选择，完善了目前信贷风控模型。

最终模型下的 AUC 值相比于银行原有单边模型提升了数个百分比。在已产生几百笔贷款的贷前审批中，已放款小微企业尚未出现重大风险案例（出现 M3+ 逾期），并预计每年可为银行降低小微企业不良贷款损失数千万元。

数牍科技：助力金融、政务等场景，打造数据要素安全流通基础设施

案例 3：基于双向隐私保护，提升保险业存量客户运营水平

传统路径上，保险公司在进行客户的存量运营时仅动用自身信息资源，然而受制于数据总量不足、维度较少等因素，缺乏充分挖掘存量客户库能力。新业务开展依赖既有数据，营销亦受限。

对此数牍科技调用了隐私计算产品，赋予保险公司与合作运营商基于双向隐私保护的数据协作能力。首先，保险公司通过隐私保护集合求交技术匹配相关用户，另一方无法留存或反推用户身份。仅当保险公司明确了需要触达的用户后，双方完成 ID 信息的交互，全程保障双方客户信息免于泄露。其次，通过纵向联邦学习，将保险公司历史投保成功标签与运营商用户画像标签相结合，从而建立基于纵向联邦学习的保险意向模型。由此完成不交换原始数据前提下，实现数据价值交叉挖掘。

在应用数牍方案建立了购险兴趣模型后，既有人群评估评分前 50% 的人群购险率提升至原先 1.8 倍。在保险营销场景中，数牍方案拓宽了数据样本量及维度，帮助保险公司高效触达存量客户，支持客户输出画像标签的精准预测从而提高了转化率。

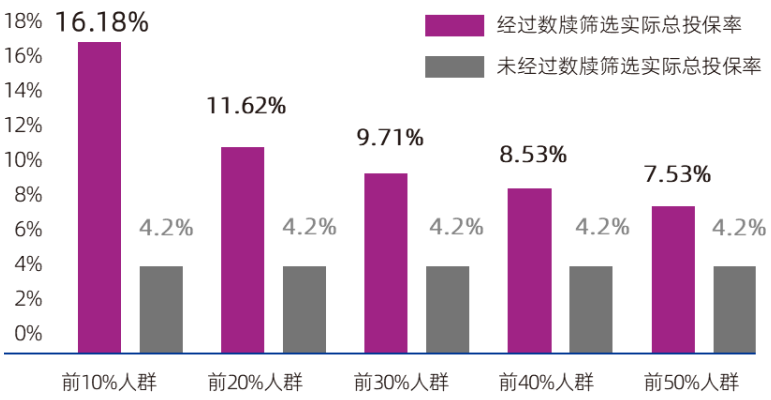

图 | 运营商-数牍-保险公司隐私数据用户意向识别结果图（来源：数牍科技）

锘崴科技：保护基因数据隐私，助力风湿病联合研究

锘崴科技团队自 2011 年起便研究隐私机密计算，于 2013 年发表全球第 1 篇医疗在线联邦学习论文，并创建了 iDASH 隐私计算大赛。锘崴科技已有数十家医院客户服务案例及运营商等伙伴，落地医疗、政务场景。在医疗领域有跨国多中心罕见病统计分析、多中心基因组分析案例。

案例概述：锘崴信隐私机密计算平台提供技术支持，由上海某三甲医院牵头，全国多家医院联合完成了一项有关强直性脊柱炎的 GWAS（全基因组关联分析）。这是全国范围内首次实现带有隐私保护计算、不分享明文个体基因数据的 GWAS 分析。

产品部署：依托锘崴科技基于隐私保护计算的高性能基因组数据联合共享和分析平台，研究团队设计开发了新框架：iPRIVATES。框架使用具有隐私保护功能的联邦学习（Privacy-preserving Federated Learning）方法连接多个数据源，研究过程只交换加密后的中间计算结果，不泄露患者级基因分型数据。在数据共享的全程保护患者信息，达到数据共享与隐私保护的双重目标。此外 iPRIVATES 框架融合多种技术和算法支持联邦 GWAS 分析的可配置管道，可灵活集成和配置不同的 GWAS，方便识别 SNPs （单核苷酸多态性）与某些重大疾病特征之间的关联。

价值成果：团队还分别通过模拟数据集和真实数据（跨多家医院的真实环境数据）两种方式来评估 iPRIVATES 性能。实验结果与传统集中式计算结果一致，以此证明平台在保护数据隐私的同时亦保障计算效果，证明锘崴平台安全可靠。

该多中心强直性脊柱炎全基因数据分析研究成果发表在生物信息学顶级期刊《Briefing in Bioinformatics》上，同时获得上海科技进步一等奖。

Chapter 4

乘势：

隐私计算乘数字化大势，数据服务市场建设掀起热潮

- 商业化现状：客户集中于“3+1”场景，开辟新数源为核心需求
- 燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

商业化现状：客户集中于“3+1”场景，开辟新数源为核心需求

1.付费客户画像：数字化程度高、数据赋能效应明显的用户使用意愿强烈

隐私计算方案付费客户拥有数字化程度较高特征：现有行业客户主要集中于金融、政务及医疗领域，这些客户汇集了数据并天然重视数据价值，他们或是现有数字化程度较高，或数字化进程正在蓬勃发展中，与此同时数据带来增益显著，有较强动力为广开数源的隐私计算产品买单。

金融业：在数字经济大潮中受到数字货币、电子支付、普惠金融、虚拟银行等不断拓展的新金融科技变革影响，金融业数字化程度已经卓见成效且仍在不断加深中。银行、保险机构可以通过广开数据源头获取更多维度、更丰富量级的数据，从而拿到更多更丰富金融风控手段和营销画像颗粒。

典型案例如小微企业贷款风控，使用隐私计算技术释放政务、运营商的数据能量，同时也不会危及到民众和客户的隐私及自身机构的利益兴趣。而随着金融科技的进一步延伸及新需求涌现，隐私计算技术将会在金融领域迸发更大的能量。

政务领域：随着政策引导下政务数据不断释放能量，政务数据的范围和质量都在不断提升。在包含企业注册登记、经营许可、公共交通、气象资料等公开数据方面，据《国家数据资源调查报告（2020）》统计，截至 2020 年底中国有各级地方政府数据开放平台 142 个，持有有效数据集多达 98558 个[32]。而在更多可能涉及隐私的数据上，随着各地大数据流通交易和监督管制的制度机构日趋完善，隐私计算辅助下的政务数据利用也将迎来更广的应用场景。

[32] 中国信息通信研究院、中国网络空间研究院. (2020). 《国家数据资源调查报告（2020）》.

商业化现状：客户集中于“3+1”场景，开辟新数源为核心需求

医疗行业：医疗数字化浪潮持续勃兴，电子病历、智能医学影像、传染病模型建构预测、健康管理等领域不断发生变革，诸多场景下的数据由于属性天然事关个人核心利益，同时数据又与病人身份息息相关，因而对隐私技术有强需求。医疗行业数字化开疆拓土存在大量机遇。

形成中的数据服务市场：隐私计算技术可分离数据的所有权与使用权，在所有权和数据隐私有保障的前提下，令供需双求方数据产生价值，因而在数据交易中占据了重要地位。以北京大数据交易所和上海大数据交易所为例，在建设过程中，业内多家隐私计算商作为技术输出方承担了重要角色，隐私计算作为服务的底层技术支持嵌入了交易所的基层架构中。

金融、政府、医疗三类机构掌握海量大数据，对数据赋能业务需求较为强烈，往往渴望更多维度、创新渠道的新数据。而正因这类机构对数据较为倚重，面临监管与合规措施不断落地的情况 ，这些机构以金融机构为代表受到掣肘最多，因而对隐私计算方案有更大需求。目前隐私计算应用场景也多集中于相关行业领域。

随着数据要素市场的进一步落地，各地涌现的数据交易平台正是当下隐私计算行业变革中尤为重要的新应用场景，并且将在近期内持续为隐私计算付费。随着数字化变革在传统领域发生及数据要素市场的进展落地，隐私计算的新场景仍在不断拓展中，在汽车出行、工业领域、农业领域等数据富集领域在中长期未来将持续拥有机遇。

2.技术使用动机：合规、拓源、降本，三股力量交织促成

数据合规需求是近年来驱动行业的核心逻辑，客户为了规避风险买单隐私计算：《数据安全法》、《个人信息保护法》等系列事关数据安全、数据隐私的法律业已出台生效，相关条例规范了行业数据利用方式。法律落地情况与行业影响虽仍旧处于摸索期，长远看受制于行业规范和新法体系持续影响，隐私计算行业的客户将有长期的合规需求：利用隐私计算技术规避违规风险，在既有的行业规范与新法律体系下合法合规地利用数据创造价值，这也是近两年来资本热潮掀起、行业声势渐长的底层逻辑。

除了新法规定，传统上金融场景也有既往受限案例，例如大型金融集团往往实控多个注册公司、横跨不同行业都有大量业务，利用隐私计算可以合理规避风险、防止敏感数据出入库，同时盘活集团生态下的经营信息、客户数据从而获取更大收益。

隐私计算赋予客户主动开拓更多数据源的能力，集成多维数据提振业务：对于使用隐私计算产品的客户而言，除了合规压力下的被动因素，隐私计算能主动拓展新的渠道和边界，利用一篮子技术对接更多以往难以释放的数据价值，在增量的维度上为企业带来效益。针对原始数据固有的易复制、易篡改属性，由此衍生带来的一旦数据本体离库便难以把控的情况，隐私计算充分赋予了数据控制权同时开放了使用权。

在挖掘多维数据源头方面，金融业落地案例产生效果尤为显著：通过开辟运营商、政务数据为银行、保险商等机构获取了存量客户群体以往所没有的数据。从风险控制角度而言，隐私计算使得银行、保险公司获取了客户较之以往更全面、细腻的信息，可充分衡量其营收能力、违债风险。在营销角度，则可勾勒精细用户画像，实现更有效率的精准营销、定向营销。

商业化现状：客户集中于“3+1”场景，开辟新数源为核心需求

利用隐私计算平台闭环交易数据，降低信任成本及交易阻力：在隐私计算成为选项前，行业内的数据交易受制于各方在数据把控方面的顾虑，因而交易量上升势头不足。数据供给方往往担忧数据流出后，相关领域业务被同质化的对方抢夺。而需求方则难以获得对方提供的数据价值衡量标准，因而交易有效性难以保障。另一方面双方都担忧业务受到对方侵蚀，由此难以产生互信关系。

这部分数据的交换需求和实现过程，在隐私计算开启前早已凸显，常见于金融科技公司的业务开展过程中，两个金融机构有数据需求、却又保有顾虑的情境。隐私计算平台的出现赋予了数据高度可控性并且在数据交易全程拥有法律效力的存证，因此很大程度上降低了交易门槛，将以往拥有的需求释放出来。

燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

1.隐私计算底层技术相对成熟，新硬件或将带来性能提升，产品化能力成为核心竞争力

隐私计算底层技术业已成熟，提高性能、提升算力或成焦点：从 1982 年姚期智“百万富翁问题”出发，安全多方计算历经数十年研究与产业积累，现有的技术能力相对成熟，并衍生出了庞杂的技术能力树。而以 Intel、ARM 为代表的可信执行环境也经过了十多年发展，在诸多领域拥有实际应用。联邦学习更是在人工智能的广泛运用中得到了众多开发者的实践。时至今日，隐私计算技术方案与基本框架已经成熟，多个技术子项各有所长拼合打包入终端解决方案中，在落地应用方面也经过了成熟的验证。

在技术方面，目前隐私计算的行业技术热点落脚于性能提升上，通过硬件资源的整合、分布式架构可提高算力、提升隐私计算效率。此外，FPGA 芯片在未来可能会给隐私计算能力带来性能上的突破，大幅提升计算能力。

产品能力、运营能力在当下厂商竞争中占据重要地位：密码学方案具有相对复杂的运算逻辑，在处理较高量级的数据时耗时较长，而联邦学习则在安全性方面有赖于与其他技术拼合，可信执行环境则受制于内存大小运算效率受限。当下的产品竞争中，如何综合运用上述方案实现匿名匹配、联合分析、联邦建模、匿踪查询等多功能，并且在实际产品运营中积累大量可复用的行业经验，并以此反哺产品建设和整体落地流程成为当下厂商竞争的重要方面。以数据服务市场建设考量，相关厂商应当持续开发面向特定需求、可复用的产品，更应当提供响应市场需求的隐私计算能力，且在后期不断打磨、形成优良的后续运营机制。

燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

2.与区块链等多技术融合、健全数据交易机制，共建数据服务市场

区块链可溯源特性与隐私计算“不可见”形成强互补：以近年来飞速拓展边界的区块链技术为代表，隐私计算相关领域的长足进展，一定程度上解决了隐私计算产业化应用过程中面临的数据利用与数据监管博弈的难题，较大程度上提振了隐私计算需求、加速行业的发展。

在区块链之前的纯密码学流程方案中，数据本身在使用过程中可以做到完全的隐私保护，然而却不利于外在的数据主体或第三方监管机构的结果验证、监督落实，数据不可见而可用在某些情况下反倒成为黑箱，使得第三方难以信任。

建设数据要素市场，隐私计算须拼合其他技术与机制：以数据市场建设为目的进行通盘考量，其中最为显著的即为区块链技术，而区块链技术在数据确权的同时也需要重视数据隐私，由此可以看到市场的一方面是主打隐私计算方案的企业纷纷开始拓展能力，引入区块链技术。另一方面诸多传统上从事区块链技术的企业，为了进入数据市场分一杯羹，也开始打造隐私计算能力，招徕密码学、联邦学习领域顶尖研发与产业人员。

数据交易是系统工程，数据质量评估体系也需建立相应共识机制。回溯以贵阳大数据交易所为代表的初代数据交易所经验，数据集本身的质量需要一定的评价机制和共识。与隐私计算技术方案相辅相成的是数据市场建设的系统性工程，为建设数据要素市场，就要建立良好的数据评估体系，以此避免数据领域的劣币驱逐良币、市场失序状况。

燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

3.“数据合规元年”，中国数据平台建设热潮是行业新增长点

系列政策扶持下，春笋般涌现各类数据平台有对隐私计算的强需求：随着数据作为生产要素在中国的进一步落实以及相关政策不断加码，大数据平台、数据交易所等机构在各地的建设逐步铺开。隐私计算技术作为充分保护数据隐私、分离数据所有权和使用权的技术集，解决了数据平台建设运营中的诸多问题，因而在这波热潮中充当了核心的技术赋能角色、具有较大商业机会。

数据本身具有易复制性的特征，对于数据所有方而言，一旦数据进入流通市场后续环节难以控制数据的数量与流向，极易造成数据的泄露、复制、篡改等后续诸多问题。通过隐私计算这一技术，数据供需双方可以通过中介交换数据价值、而无需获取数据集本身，因此一方面对数据的交易定价有利，另一方面则免除数据的次生问题，提升了数据交易可控性。

燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

在数据平台建设流程中，隐私计算厂商提供了技术方案深度参与建设，提供包括前期需求对接、中期技术落地调试、后期长期运营支持等多方面工作。因此在未来一段时间内，隐私计算行业机遇将会与这一波数据平台建设热潮息息相关。

数据中心：国家发改委等部门在 2021 年 5 月联合印发了《全国一体化大数据中心协同创新体系算力枢纽实施方案》，针对各地各级政府纷纷发展大数据中心由此产生了一定程度的资源冗余、机构重叠现状做出指示。方案规划了城市级、区域级、全国级三个层级的大数据中心建设体系，分别对应延时要求极高、较高、不高的数据类型。自此，全国性的数据中心建设有了清晰的全盘方案有序展开。

隐私计算在数据利用过程中，尤其在前两个级别具有较高需求，在已经成熟的金融、汽车领域应用，及中期内工业互联网应用上具有较高的实用价值。

数据交易所：在 2021 年 3 月、11 月北京国际大数据交易所和上海数据交易所分别成立，在部分行业人士称为“数据合规元年”的节点上成立，两大数据交易所在促进数据要素充分流通、数据确权并充分提振数字经济工作上，开辟了重要的中心节点平台。而北京国际大数据交易所在成立之初，便强调推动数据交易底层技术创新。且针对权属不清、信息泄露危险，该所更是直接强调要依托北京隐私计算、区块链技术领域的先发优势分离数据所有权与使用权，实现数据“可用不可见”。

燎原之势：工程化能力成行业焦点，数据服务市场为行业新机遇

4.现有行业玩家逐渐分化，隐私计算或拓展至工业互联网等领域

厂商逐渐分化为底层技术供应商、终端方案商，共同对外输出隐私计算能力：随着隐私计算落地领域逐步拓展，应用场景从最初的银行、保险、政务、医院深入数据服务市场。或拥有渠道优势或拥有技术优势的厂商开始在行业竞争中分化，按照各自的资源禀赋逐渐锚定市场位置，由此市场分层已经初见趋势：

- 隐私计算技术供给公司：专注于研发与提供底层隐私计算软硬件产品。在竞争力维度上，集中优势专注于技术的精进打磨，不断降低产品成本、提升性能与处理效率，为数据服务市场提供优质的产品性能。

- 数据市场服务公司：该类公司立足于数据服务终端场景，面向客户专注从事顶层落地产品研发及后续运营打包方案落实，在产品侧不断打磨隐私计算方案的易用程度、综合工程性能以及控制成本，在运营侧针对特定行业客户调试方案，深化客户理解从而在服务市场占据立足之地。

中长期内，随着数据交易蔚为大观，隐私计算将拓展至工业互联网等领域：隐私计算出现的核心领域是数字化程度高且数字增益效应明显的行业，在当下主要涉及金融等领域。而随着数字化浪潮席卷拓展至更多行业，隐私计算与之相伴而盛。从中长期未来看，工业互联网、农业互联网将会存在机遇。而在机制上，伴随着数据交易、数据服务的落地，隐私计算作为能够释放数据价值、明确数据权属的核心技术，将会在更大量的场景下提供服务能力。届时，隐私计算在性能、产品化等方面又将生成更大的变革。

结语

隐私计算相关科技研究由来已久，上溯至上世纪 80 年代由姚期智的密码学经典发问开始，历经漫长研究历程，而后逐步工程化落地实践。随着数字化浪潮勃兴、人工智能渐起，在近年来数字经济蓬勃增长的情况下，因其赋予数据利用的能力而得以逐步在业界生根落地。

与海量数据相伴相生的则是数据安全、数据隐私问题。尤其在数据隐私方面，近年来行业相关趋势是逐步从关注数据隐私的社会思潮落实为法律法规具有强制效力的要求。在业界则产生了实在的数据利用壁垒，因而生成了大量合规需求。

一方是增加数据维度、拓展数字边界的拉力促使隐私计算相关技术入场，而另一方则是时下积极推动的各类监管措施及细化的数据要素市场建设指导，进一步推动了隐私计算技术合集应用边界。

随着机制、机构的积极建设与数据要素市场的日渐成型，隐私计算热潮将长期持续。当数据权属日渐明晰，数据交易日益兴盛，大范围的数据的流动行业生态将逐步成型。这一波红利已经行至眼下，业界目光正在聚焦相关的规划。而长远看，紧贴数据的隐私计算行业则将在更多数字化升级落地领域推广应用。

最后感谢以下产业专家与技术专家接受调研：洞见科技创始人兼董事长姚明先生、瑞莱智慧首席架构师徐世真先生、锘崴科技创始人兼董事长王爽先生、数牍科技联合创始人兼CTO蔡超超先生与副总裁张迎春先生。 *（注：上述排名不分先后）*

参考文献

Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity* . Springer Nature.

Future of Financial Intelligence Sharing (FFIS). (2021). *Innovation and discussion paper: Case studies of the use of privacy preserving analysis to tackle financial crime*.

Kaitlin Asrow, Spiro Samonas. (2021). *Privacy Enhancing Technologies: Categories, Use Cases, and Considerations*. Federal Reserve Bank of San Francisco.

Royal Society (Great Britain). (2019). *Protecting privacy in practice: The current use, development and limits of privacy enhancing technologies in data analysis.*

The Privacy Preserving Techniques Task Team (PPTTT). (2018). *UN Handbook on Privacy-Preserving Computation Techniques.*

World Economic Forum. (2019). *White Paper: The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value.*

版权声明

免责声明

本报告投融资数据及部分企业数据来源于 CB Insights，报告所载数据和观点，仅反映 CB Insights 中国基于发出此报告日期当日的判断。CB Insights 中国对报告所载数据和观点的准确性、完整性不作任何保证，对该报告的数据和观点不承担法律责任。

不同时期，CB Insights 中国可能会发布其它与本报告所载资料、结论不一致的报告。同时，CB Insights 中国对本报告所载信息，可在不发出通知的情形下做出修改，读者应自行关注相应修改。

关于 CB Insights 中国

CB Insights 成立于 2008 年，将数据科学、数据可视化和预测分析工具相结合，为VC/PE、跨国企业、初创公司等创建了一个技术和行业研究的全球化数据平台。CB Insights 是全球知名创投研究机构、硅谷最强智库之一、最经常被媒体引用的投资数据公司以及知名市场研究机构。

2019 年，CB Insights 与 DeepTech 合作落地在中国，并以 CB Insights China （CB Insights中国）为主体扎根技术和行业研究，研究领域覆盖人工智能、生命科学、半导体、新能源汽车、金融科技、零售消费等十余个领域、几十个细分赛道，致力于发掘行业中更多有潜力的科技企业。

如有任何研究与合作需求，请联系我们：cbinsightschina@deeptechchina.com。

关于 DeepTech

DeepTech 成立于 2016 年，是一家专注于前沿新兴科技的新型赋能与传播机构，服务科学家以及城市、园区、企业、科研院所、资本等新兴科技生态网络，通过产业服务、数据赋能、科学资本实验室 (Venture Lab) 及科技出版服务四大业务板块，推动科学与技术的创新进程。

CBINSIGHTS | CHINA