隐私计算技术对数据开发利用的突破与限制

作者：潘永建 | 朱晓阳 | 左嘉玮

引言

数字经济时代，数据已成为重要的生产要素，收集、使用和分析数据的规模和速度正在迅速增加。然而，出于数据安全和个人信息保护方面的考虑，数据共享的落地仍进展缓慢。因此，为打破“数据孤岛”，充分释放数据的价值，隐私计算技术应运而生。

根据联合国大数据全球工作组的定义，隐私计算(Privacy-Preserving Computation)是指可在保证原始数据加密或者不可见的状态下、对数据进行计算和分析的一系列技术，包括安全多方计算、同态加密、可信执行环境、差分隐私、联邦学习等[1]。在隐私计算中，原始数据不会离开“所有者”，各参与方只分享最终的计算结果，实现了数据“所有权”与使用权的分离，从而可以最大限度挖掘数据要素的价值，为数据融合需求与隐私保护要求提供了解决方案。

一. 隐私计算主要技术

隐私计算技术的核心思想是通过代码加密、算法等方法，构建数据共享的信任基础。当前，行业技术主要可以分为三类:

- 密码学技术：以安全多方计算、同态加密为代表，通过算法对原始数据进行加密或分割，保证数据接收方无法识别。
- 可信执行环境：基于硬件的防护能力构建一个安全区域，将需要保护的数据汇聚到该区域后进行计算。
- 联邦学习：隐私计算在人工智能领域的最新应用，多个参与方之间无需共享训练数据，只传输模型参数，从而实现在原始数据不离开企业私有域的前提下，进行联合建模。

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

[1] Bigdata UN Global Working Group. UN Handbook on Privacy-Preserving Computation Techniques.

此外，差分隐私技术可适用于隐私计算结果的发布，在广义上也属于隐私计算技术的一种。它通过添加噪声[2]的方法来达到隐私保护的效果，从而确保攻击者无法根据输出差异来推测特定个体记录的信息。

(一) 安全多方计算

安全多方计算主要研究“在无可信第三方的情况下，如何安全地计算一个约定函数”的问题。《多方安全计算 金融应用技术规范》将其定义为“一种基于多方数据协同完成计算目标，实现除计算结果及其可推导出的信息之外不泄漏各方隐私数据的密码技术。”[3]

安全多方计算常用的密码技术有混淆电路、不经意传输、秘密共享、同态加密等。通过运行安全多方计算协议，多个参与方可以在不暴露数据明文的情况下进行协作，共同对数据执行计算，当协议完成时，各参与方只知道自己的输入和计算结果，而无法获知其他参与方的输入。安全多方计算适用于多个参与方希望联合对数据进行计算，但出于数据安全和隐私保护考虑而不能直接共享数据的情形。例如，安全多方计算可以允许竞标者识别谁赢得了拍卖，而不透露任何关于实际出价的信息。

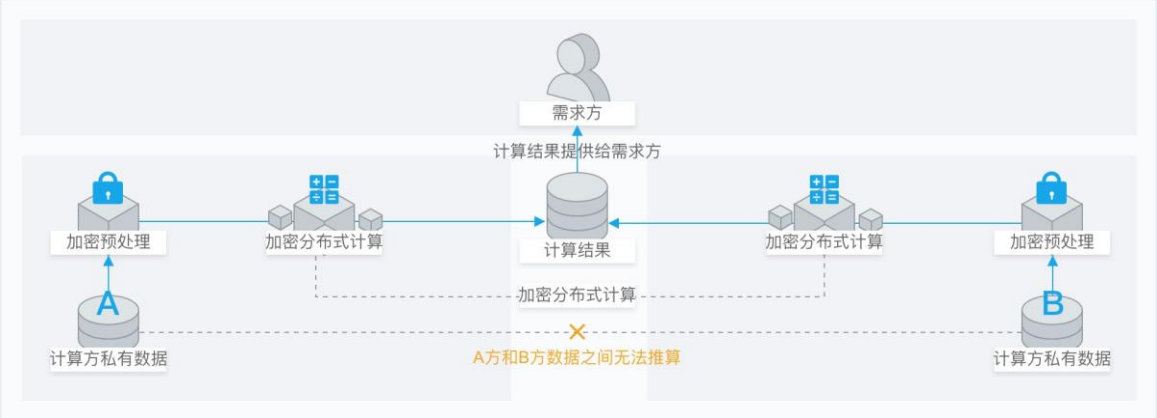

图 1-安全多方计算架构

来源：富数科技

(二) 同态加密

同态加密是指满足密文同态运算性质的加密算法，它允许对加密数据(密文)进行计算得出加密结果，解密之后，与直接对原始数据(明文)计算的结果一致。

同态加密不需要对加密数据进行解密就可以对其进行计算，适用于数据处理过程外包给第三方组织(如云服务商)的情形。它可以让用户在保障数据隐私的前提下，充分利用云服务商的计算资源。

[2] 噪声是指对数据集中的数据值(如个人标识符)进行随机变化

[3] 《多方安全计算金融应用技术规范》(JR/T 0196-2020)第 3.1 条。

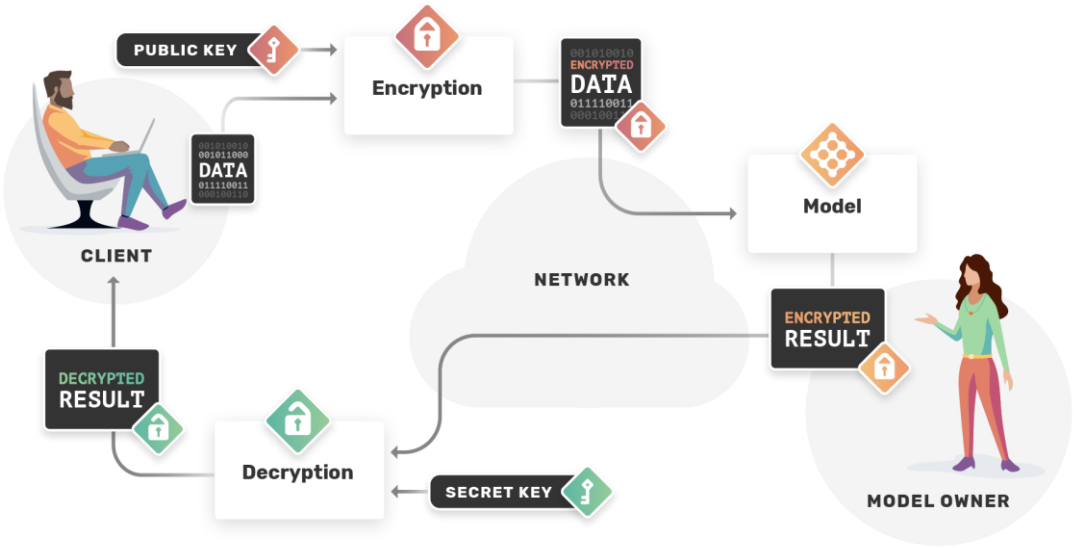

图 2-同态加密架构

来源: Openmined

(三) 可信执行环境

可信执行环境是一种基于硬件和操作系统的安全架构，它将运行在其中的数据与通用执行环境隔离，以保障数据的机密性。当需要进行隐私计算时，通用执行环境将加密的数据送入可信执行环境，解密为明文后再进行计算。

可信执行环境提供了一种基于硬件保护能力以实现数据隐私保护的方案，其安全性依赖于硬件设备自身的安全性，因此在实际使用时需要选择可信任的硬件厂商或平台服务商。

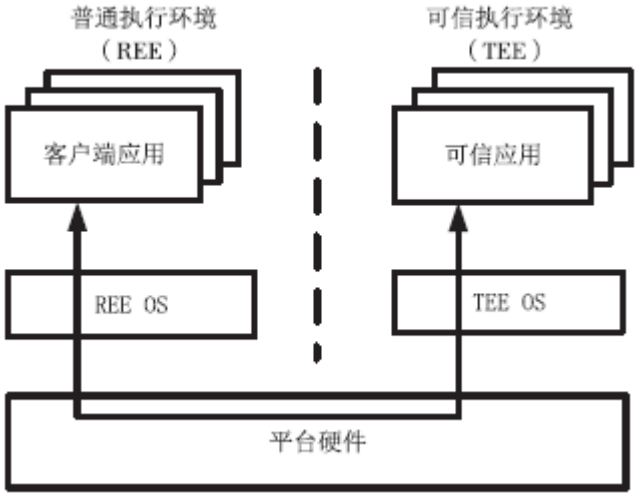

图 3-可信执行环境架构

来源: 《信息网络安全》期刊

(四) 联邦学习

联邦学习是一种分布式的机器学习框架，联邦学习可以在多个参与方不披露自身原始数据的情况下，实现联合建模。

在传统的机器学习框架中，多个参与方需要将各自持有的数据集中到一个数据中心，用来训练模型。在联邦学习框架下，多个参与方利用自有的原始数据训练机器学习子模型，并通过加密机制传输中间结果(如梯度)，最终建立并维护一个共有的模型，这样不仅保护了各参与方的数据隐私，还降低了大量数据集中传输的成本。

图 4-联邦学习架构

来源：微众银行 《联邦学习白皮书》

(五) 差分隐私

差分隐私根据部署模式可分为中心化差分隐私和本地差分隐私:

- 中心化差分隐私的噪声机制主要以拉普拉斯机制和指数机制为主，数据控制者在发布数据集对统计结果上添加以零为中心分布的随机值，确保单个记录的存在与否不会对查询结果产生重大影响。

- 本地化差分隐私的噪声机制主要以随机响应为主，用户在本地对数据添加噪声以后，再发送给数据控制者，在数据聚合时，由于噪声符合一定的概率分布，因此不同记录间的噪声可以相互抵消。

差分隐私建立在坚实的数学基础之上，能够在实现数据集价值的同时，保证特定个人信息主体不被识别，是当下比较主流的隐私保护技术之一，例如谷歌公司正是使用基于布隆过滤器和随机响应技术的 RAPPOR 本地差分方案，从 Chrome 浏览器中收集用户的行为数据。

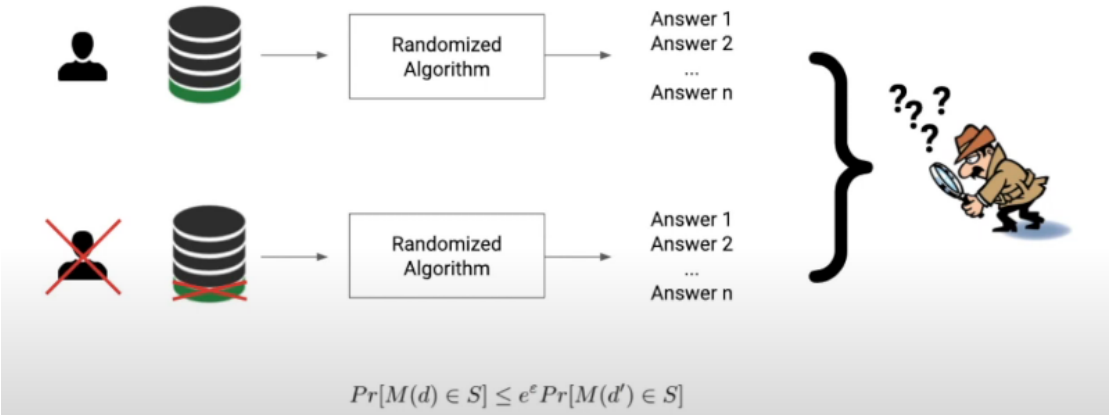

图 5-差分隐私架构

来源: Dwork et al.

二. 隐私计算可以满足匿名化要求吗

我国《网络安全法》第四十二条、《民法典》第一千零三十八条均为对外提供个人信息设定了“经过加工无法识别特定个人且不能复原的除外”的例外情形，《个人信息保护法》(以下简称“《个保法》”)第四条亦明确规定，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”。

因此，企业往往致力于寻找一种技术手段来实现个人信息的匿名化，从而一劳永逸地解决数据合规问题。也就是说，在初始阶段完成合法的数据收集后，后续的存储、处理、分析等阶段不再需要承担额外的个人信息保护义务。近年来兴起的隐私计算技术为解决这个问题带来了希望，拥护者们认为，隐私计算可以通过以下两个路径规避个人信息合规风险:

- 在共享之前对个人信息进行预处理，如加密或者转换(分割、添加噪声等)，使其无法重新识别出特定个人并且不能复原。
- 尽可能减少个人信息的披露，在本地对原始数据进行计算或分析，仅对外传输中间结果，而后者已不再属于个人信息。

那么，隐私计算真的能在法律层面上实现个人信息的匿名化吗?

(一) 区分去标识化与匿名化

《个保法》对于匿名化与去标识化的定义与《信息安全技术 个人信息安全规范》(以下简称“《个人信息国标》”)一脉相承:

- 去标识化，是指个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。
- 匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。

两者均是通过技术手段对个人信息进行处理，去除信息与个人信息主体之间的关联性，使其无法识别特定自然人。区别在于，匿名化的处理更为彻底，要达到“不能复原”的效果。根据《信息安全技术 个人信息去标识化指南》列出的常见重标识方法，符合匿名化标准的技术至少应对以下三种识别威胁具有很强的抵抗力:

- 隔离: 基于是否能唯一确定一个个人信息主体，将属于一个个人信息主体的记录隔离出来;
- 关联: 将不同数据集中关于相同个人信息主体的信息关联;
- 推断: 通过其它属性的值以一定概率推断出一个属性的值。

需要指出的是，由于数据科学领域也存在诸如假名化、去标识化、匿名化等术语，因此，在实践中，企业往往将这些方法与法律语境下的匿名化相混淆，认为去除个人信息中的直接标识符(姓名、身份证号等)就可以实现匿名化。事实上，许多传统的去标识化方法都存在被重新识别的可能，无法达到匿名化的效果。特别是随着大数据时代的到来，多源数据的融合进一步加剧了个人信息的重识别风险。例如, 2006 年, Netflix 举办了一场电影推荐算法大赛，同时发布了“经过匿名化处理”的用户数据集供参赛者训练算法，仅保留每个用户对电影的评分和评分的时间。但是，研究人员发现，将 Netflix 匿名化的数据库与 IMDB 数据库结合之后，可以重新识别出部分用户的身份信息。[4]Netflix 不得不取消该比赛，并因此受到了高额罚款。

(二) 隐私计算的匿名化认定

尽管《个保法》《个人信息国标》给出了匿名化的定义，但是并未明确规定其认定标准。从技术角度来说，或许不存在绝对“不能复原”的数据，否则这样的数据也失去了可用性。鉴于此, GDPR 对可识别性的判断采取了一个相对缓和的标准，只需考虑所有可能合理使用的识别方法，检验合理性的因素包括现有技术和实施成本等。[5] 2020 年，欧盟地平线 “Scalable Oblivious Data Analytics" (SODA)”项目对隐私计算技术进行了研究，认为“通过秘密共享、差分隐私等技术，可以去除个人数据的可识别性，将其转换为非个人数据。”[6]2021 年，中国信通院发布的《隐私保护计算与合规应用研究报告》也指出，“当启用了最先进的加密技术，且执行了严格的密钥管理，

[4] Arvind Narayanan, Vitaly Shmatikov. Robust De-anonymization of Large Sparse Datasets. IEEE Symposium on Security and Privacy.
[5] GDPR Whereas:(26)
[6] EU Horizon2020 "Scalable Oblivious Data Analytics" (SODA), Deliverable D3.5.

数据接收者无法获取解密密钥，在当前经典计算机的算力下，在一定的时间期限范围内想要破解几乎又是不可能的，则可认为构成匿名化。”[7]

遗憾的是，虽然理论上隐私计算可以保障数据的安全性，但在实际应用中，企业通常会为了性能而做出妥协。比如，为了提高计算效率，多数安全多方计算框架都仅实现了“半诚实模型”[8]的安全性，而实际中的情况往往更为复杂，当出现恶意的参与者时，很可能会发生数据泄露的风险。在联邦学习中，尽管不需要传输原始用户数据，但研究表明，攻击者可以通过模型的中间参数推测出原始信息。[9]部分前沿的联邦学习协议已经可以做到不披露中间结果，只披露最终模型，从而实现更好的安全性，但是在性能还有很大的提升空间。

因此，在目前阶段，企业不宜简单地将隐私计算和匿名化划上等号，应当审慎评估所使用的隐私计算技术是否符合“无法识别、不能复原”的要求。此外，除了技术手段，企业还应采取强有力的组织措施，以防止个人信息的重新识别。例如制定隐私安全策略和规程、定期开展员工安全培训、组织员工签署保密协议等。

三. 隐私计算的积极意义

如前文分析，鉴于判断标准的模糊，目前仍不能明确隐私计算是否符合“匿名化”的要求。但可以肯定的是，通过实施隐私计算，可以在一定程度上降低数据主体的风险、帮助企业履行数据合规义务。

(一) 符合数据最小化原则

根据《民法典》第一千零三十五条规定，“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理”，《个保法》第六条规定，处理个人信息“应当与处理目的直接相关，采取对个人权益影响最小的方式”。

安全多方计算、同态加密等隐私计算技术可在原始数据保留在本地的前提下，实现各参与方之间的协同计算，从而确保各参与方在整个数据处理过程中无法获知计算结果之外的信息；而联邦学习系统不需要收集和处理原始的训练数据，只需要从每个参与方收集本地模型参数以更新全局模型。这些隐私计算技术仅收集和处理与描述的目的直接相关的、有限的个人信息，遵循了数据最小化原则。

[7] 中国信息通信研究院《隐私保护计算与合规应用研究报告 2021》

[8] 安全模型可分为半诚实模型和恶意攻击模型两类。半诚实模型是参与方在接触和处理其他参与方隐私数据时，在严格遵守协议规范基础上，尽其所能地从接触和处理的数据中挖掘出有效信息；恶意攻击模型是参与方可能做出任何行为，尽其所能地获得关于隐私数据的有效信息，如背离协议或与他人串通等，这样的参与方也称为不诚实参与方。

[9] Li Z, Huang Z, Chen C, et al. Quantification of the leakage in federated learning.

(二) 可帮助企业履行数据合规义务

根据《数据安全法》第二十七条规定，开展数据处理活动应当采取相应的技术措施和其他必要措施，保障数据安全。采用隐私计算技术无疑可以减少数据泄露的风险，从而提高企业的数据安全水平。因此，使用隐私计算可作为企业履行数据安全保护义务的证明。

此外，根据《个保法》第六十九条规定，“个人信息权益因个人信息处理活动受到侵害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”在发生个人信息安全事件时，采用隐私计算可在一定程度上证明企业自身没有过错，作为减轻或免除责任的依据。

四. 面临的主要挑战

(一) 仍需遵循个人信息保护原则

根据《个保法》第四条第二款，“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。”去标识化过程本身既构成法律意义上对个人信息的“处理”，因此，即便将隐私计算技术处理后的数据视为匿名数据，对于原始数据的处理仍需受到知情同意、目的合理等个人信息保护原则的约束。

现阶段，个人信息主体的知情同意是企业处理个人信息的常用法律基础，企业有义务明确告知用户使用隐私计算的目的、具体的处理方式和范围。但由于隐私计算涉及密码学、人工智能等多个领域，而大多数用户不具备相关的专业知识，难以理解和信任隐私保护的算法逻辑。因此对于企业而言，让用户信任并接受隐私计算的安全性将是一项很有挑战性的工作。为解决这一问题，业界正在努力推进隐私计算相关标准的制定，以提高隐私计算技术的公信力，相信在将来，隐私计算会被越来越多的用户所接受。

此外，根据技术中立原则，隐私计算技术的目的是否合理取决于企业自身商业模式的合法性。因此，在实施隐私计算时，企业仍需审查数据处理目的，例如是否有益于社会、是否会对某些个人或群体造成不利影响等。

(二) 在数据保护和效用之间权衡

为了实现数据保护的目的，在使用隐私计算时往往需要付出一定的效用成本。

- 在差分隐私中，将噪声添加到数据集中会导致一些有用信息的丢失，因此在准确性方面需要付出一定的代价。差分隐私的数据保护水平由隐私预算 ε 决定，ε 越小，数据保护水平越高，但相应的数据可用性也就越低，企业需要对隐私预算进行合理地控制。
- 对于在加密数据上进行计算的隐私计算技术，如同态加密和安全多方计算，其效用代价主要是计算量和通信量的开销。恶意的参与方会尽可能地获得关于隐私数据的有效信息(如背

离协议或与他人串通等)，因此恶意模型下协议的复杂程度和开销与半诚实模型相比，存在数量级上的差异。

因此，在部署隐私计算时，企业需要基于具体的应用场景和采用的技术，在数据保护和效用之间进行权衡。并且，由于重标识技术以及重标识攻击能力都在不断发展，企业应根据情况变化或定期进行重标识风险评估，持续监控技术的去标识化效果，以保障个人信息安全。

结语

作为一种新的技术体系，隐私计算为数据融合与隐私保护的迫切需求提供了一个相对可行的技术解决方案，在金融、医疗、政务等领域都已经实现了落地应用。但是目前隐私计算技术尚处于起步阶段，还存在着诸多问题，相关的行业标准仍处于探索的过程。总体而言，隐私计算可以有效降低数据处理活动中的隐私泄露风险，从而为用户提供更多的安全保障。但需要注意的是，企业应当在合法合规的前提下使用隐私计算技术，而不应将其视为一种规避监管的手段。

作为大数据产业发展的要素和基础，数据的开放与共享是大势所趋。隐私计算致力于实现数据的“可用不可见”，与国际隐私保护实践中倡导的“通过设计保护隐私(privacy by design)”理念相一致，具有广泛的应用前景，相信在今后会有进一步的发展。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野