隐私计算联盟
Privacy Preserving Computing Alliance

云大所
CAICT

隐私计算
法律与合规研究白皮书
（2021 年）

隐私计算联盟

中国信息通信研究院云计算与大数据研究所

2021年12月

引　言

自党的十九届四中全会将数据列为生产要素以来，数据的开放共享、交换流通成为大数据产业发展的重点。快速发展的隐私计算等数据流通新技术为产业“破局”提供了关键思路，成为建设和完善数据要素市场的重要抓手。**隐私计算**（Privacy-preserving computation）是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一系列信息技术，实现数据在流通与融合过程中的“可用不可见”。

从隐私计算实现的目标来看，能实现隐私保护的同时支持数据价值分析的技术方案都可被列入隐私计算的范畴。其中典型的技术路线包括**多方安全计算**（Secure Multi-party Computation ，MPC）是多个参与方基于密码学技术共同计算一个目标函数，保证每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入和输出数据的技术；**联邦学习**（Federated Learning，FL）可以实现在本地数据不出库的情况下，通过对中间加密数据的处理来完成多方对共享模型的机器学习训练；**可信执行环境**（Trusted Execution Environment，TEE）是将软硬件方法构建的安全区域与其他应用和操作系统隔离开，使得操作系统和其他应用无法访问或更改该安全区域中的代码和数据，从而达到保护敏感数据和代码效果的技术；**同态加密**（Homomorphic Encryption，HE）是基于数学难题的计算复杂性理论的密码学技术，能确保在密文上直接进行计算后对输出进行解密，得到的结果和直接明文计算的结果一致。**零知识证明**（Zero

—Knowledge Proof，ZKP）是基于密码学技术，证明者能在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的；**差分隐私**（Differential Privacy，DP）是通过对数据集添加噪声，避免相邻两个数据集在发布聚合计算结果时单条数据记录的泄露。

数字经济兴起以来，各国通过法律法规和国际条约来规范数据的采集和使用，提出了授权同意、匿名化、安全审查等一系列合规要求，其目的在于保障国家安全、市场竞争秩序、个人隐私、人身及财产安全、个人数据自主权利等法益。在数据合规日趋收紧的背景下，隐私计算提供了合规前提下充分挖掘数据价值、促进数据流通的一种可行的技术解决方案。但与此同时，如何评估隐私计算技术及产品的合规性、如何约定参与方的权利义务以及如何规避法律风险等问题也成为行业普遍关心的热点话题。

本白皮书从隐私计算的合规意义和常见的误区入手，对隐私计算的参与方及相互间的法律关系进行定义和分析。在此基础上，详细分析了隐私计算参与方应关注的法律和合规要点，并给出相应安全和合规方面的建议。为进一步分析隐私计算的合规提升效果，我们对广告营销、企业融资风控、个人信贷风控和人脸识别四个场景的技术方案及其隐私保护效果进行了分析。最后，基于隐私计算发展的现状和未来的需求，产业和监管的互信互动将有助于进一步推进隐私计算乃至数字经济的发展，本白皮书通过对产业的健康发展进行展望，以期隐私计算为数据价值的挖掘和国民经济的发展带来更大的价值。

版权声明

隐私计算联盟
Privacy Preserving Computing Alliance

编写委员会

❖ **主要编写单位**（排名不分先后）：

中国信息通信研究院云计算与大数据研究所

清律律师事务所

华控清交信息科技（北京）有限公司

蚂蚁科技集团股份有限公司

上海富数科技有限公司

同盾科技有限公司

北京德和衡（上海）律师事务所

中移动信息技术有限公司

中国联合网络通信有限公司研究院

北京数牍科技有限公司

联易融数字科技集团有限公司

❖ **参与编写单位**（排名不分先后）：

北京市竞天公诚律师事务所

京东科技控股股份有限公司

❖ **编写组主要成员**（排名不分先后）：

仵姣姣	闫　树	吕艾临	侯　宁
熊定中	庄媛媛	靳　晨	王云河
彭　晋	白晓媛	昌文婷	方　竞
姜　康	彭宇翔	孟　丹	娄　鹤
陈国彧	朱明烨	范东媛	王　鑫
曹　咪	张立彤	史金雨	金银玉
单进勇	陈永侠	陈　曦	魏　凯
孙中伟	李　帅	袁立志	朱　垒

隐私计算联盟
Privacy Preserving Computing Alliance

目 录

第一章

隐私计算的合规意义

2021 年《数据安全法》与《个人信息保护法》的出台，与《网络安全法》一同形成了数据合规领域的“三架马车”，这标志着数据合规的基本法律架构已初步搭建完成。在此基础上，关注重点行业、新兴技术的法律和司法解释也在今年密集发布，一方面为产业、技术的发展提供了更为清晰的指引，另一方面也意味着监管强度日渐收紧、合规压力日益凸显。因此，不同行业、不同主体间的数据融合流通面临较大的合规压力，平衡数据价值挖掘需求和满足合规要求成为数据流通产业急需解决的问题。

(一) 隐私计算有助于提升数据合规

《数据安全法》第三条指出，“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”。第七条也表明，“国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展”。可以看出，数字经济的发展需要在保护数据安全的基础上发挥数据的使用价值。隐私计算技术得

以在不转移或泄露原始数据的前提下，实现数据融合“可用不可见”的效果，为数据要素的融合流通提供了一种可能的合规“技术解”。

1.隐私计算有助于履行安全保障义务

隐私计算可作为防止未经授权访问、减少个人信息泄露、篡改和丢失的一种技术手段，还可以实现在不获知其他参与方原始数据的情况下处理数据。因此，**隐私计算可被理解为是一种加强数据安全的技术措施**，有助于保障数据处理过程中各方的数据安全，为防范安全风险提供技术支撑。

从法律层面而言，应用隐私计算也属于履行法律要求的数据安全保护义务，有利于优化数据应用安全环境和维护相关数据主体的权益。我国相关主要法律条款如表 1 所示：

网络安全法
第四十二条 **网络运营者不得泄露、篡改、毁损其收集的个人信息**；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。 **网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。**在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。
数据安全法
第二十七条 **开展数据处理活动应当依照法律、法规的规定，**建立健全全流程数据安全管理制度，组织开展数据安全教育培训，**采取相应的技术措施和其他必要措施，保障数据安全。**利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。
个人信息保护法

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。 第六十九条 处理个人信息侵害个人信息权益造成损害，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。

表 1：数据安全义务相关法律条款

2. 隐私计算有助于防止数据滥用

《个人信息保护法》确立了个人信息处理的“最小必要”原则，该原则应当贯穿数据处理的始终。“最小必要”原则可被理解为要求企业和公共机构等数据处理者以实现产品和服务目的为标准，在功能可实现的前提下保持克制，在最小范围内收集并使用个人信息。个人信息采集阶段的“最小必要”合规要求较容易达到，例如将产品使用功能框定在具体范围内、梳理需要采集的数据目录，并严格将数据采集限制在目录范围内等等。但数据使用环节的“最小必要”要求则较难达到，同时也往往因缺乏事中、事后的监督与审计机制而难以对数

据的后续失控流转追责。

数据的“可用不可见”能够有效防止数据明文在使用时被复制而导致的数据滥用，得以保证数据的机密性和完整性。例如多方安全计算运用密码学算法对数据进行密文计算，可信执行环境等机密计算使用软硬件方法构建的安全区域保护其中的数据。如果可信执行环境中的代码是按照最小必要的原则设计的，那么基于可信执行环境的技术方案也是可控的、能够满足最小必要原则的。在此基础上，参与方可以实现对每一次的数据使用进行授权，在授权后再由各参与方共同签订合约，明确算法逻辑、数据用量和使用次数，控制数据滥用，成为数据使用过程中践行“最小必要”原则的技术解。

3. 隐私计算有助于实现一定条件下的匿名化

根据《个人信息保护法》，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。从定义而言，绝对的匿名化是指无论关联多少数据都无法识别个人、无论采用何种技术都不能复原个人信息的状态。然而，在现有技术发展水平下，绝对的匿名化在统计等场景外暂时无法实现，绝对的匿名化也会大大减损数据的使用价值，可能将导致数据在大多数应用场景中无法使用，这与《个人信息保护法》中“促进个人信息合理利用”的原则存在一定程度的抵触。因此，**匿名化应当是在一定条件下（例如在可实现的算力、合理时间范围内等）的相对匿名化。** 换言之，当一种技术方案能够实现还原部分原始数据所需要的时间、算力等成本远远超出使用该部分数据可能获得

的价值时，我们认为这种技术方案已经实现了事实上的相对“匿名化”。

使用隐私计算技术本身不需要对数据进行事先的匿名化处理，但隐私计算技术可作为匿名化技术方案的一个组成部分。多方安全计算、同态加密、零知识证明和差分隐私等技术能够实现输入数据和输出数据的隐私保护，是实现相对匿名化的有效手段。此外，结合了数据加密、去标识化、可信执行环境、访问控制等技术的综合解决方案，通过构建可信受控的计算环境，对个人信息进行去标识化、加密等处理，使所有的计算均基于处理后的数据展开，并通过技术手段对试图关联或还原个人信息的高危行为进行拦截，可以实现数据计算过程中的“可算不可识”；在计算结果输出时，在可信受控环境中对计算结果进行差分隐私、泛化等处理，有助于保障数据在非受控环境下无法重识别，全方位降低隐私泄露和重标识风险，实现在一定条件下的匿名化。

4. 隐私计算有助于减轻授权同意的合规隐患

以个人数据为例，在传统中心化的建模中参与方可以获取到各方的原始数据。因此，可能接触到原始数据的所有参与方都应当受到个人信息保护的诸多复杂限制。授权同意是实践中个人数据使用最主要的合规基础之一，复杂、高昂、难落地的授权同意合规负担一定程度上阻碍了数据的流通。**包含隐私计算的技术方案有助于降低参与方在数据融通中的授权同意压力**，两种技术方案的授权同意模式如图 1 所示。

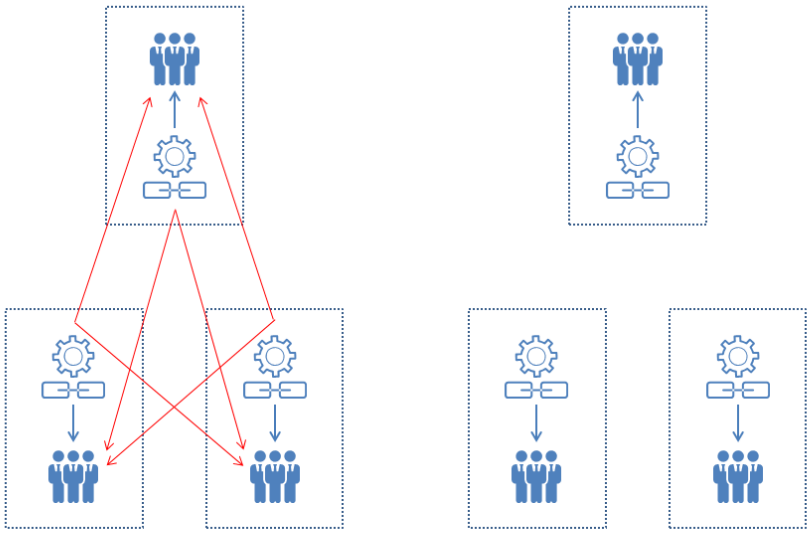

图 1 两种技术方案授权同意的差异

在隐私计算中，假设获取数据的一手数据源首先获得了个人信息主体没有权利瑕疵的授权同意，或在获取数据后对数据进行的脱敏、加密处理使计算数据满足了法律要求的匿名化要求，那么输入模型的数据不再属于个人信息的范畴，此后其他参与方对数据的计算和分析也因此可能不再需要经过个人信息主体的重复授权，从而减少了数据流通过程中由授权引发的法律风险和成本支出。

为了进一步降低合规风险，我们仍建议参与方在选择授权同意作为主要合规基础时，根据具体涉及数据的类型和敏感程度，将授权同意与去标识化/匿名化的技术方案加以有机融合，在数据流通的全流程综合降低合规风险。

授权同意涉及的主要法律条款如表 2 所示：

网络安全法
第四十二条之一

网络运营者不得泄露、篡改、毁损其收集的个人信息；<u>未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。</u>
民法典
第一千零三十八条之一 信息处理者不得泄露或者篡改其收集、存储的个人信息；<u>未经自然人同意，不得向他人非法提供其个人信息，但是经过加工无法识别特定个人且不能复原的除外。</u>
个人信息保护法
第四条 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，<u>不包括匿名化处理后的信息</u>。 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。

表 2 我国授权同意相关法律条款

5. 隐私计算有助于开发数据的使用价值

在数据确权这一核心问题尚未得到解决的前提下，企业等市场主体的积极性因其在数据生产、数据管理方面投入的劳动成果难以得到法律认可而受到一定程度的制约，主体是否对其所有的数据享有所有权等问题也使部分企业迫于合规风险而不敢、不愿参与数据流通。

隐私计算有助于在不对数据现有控制状态产生影响的基础上，满足数据流通的现实需求。以多方安全计算为例，多方安全计算能够实现在不获取明文数据的前提下利用数据的使用价值，即在保证原始数据控制权不发生改变、保证数据所有者权益的前提下传递数据的使用价值。在当下数据权属问题较难明确的前提下，通过“可用不可见”的技术方案将数据的使用价值分离出来，由此为后续数据的使用和交易提供技术基础。

对此，欧洲已有实践先例。2015 年，爱沙尼亚应用研究中心（CentAR）对大学期间工作与未能按时毕业之间的关联性进行研究。

CentAR 使用了基于 MPC 的解决方案，将个人纳税数据库和高等教育数据库中的数据进行关联和分析,并使最终输出的统计数据不包含个人信息。爱沙尼亚数据保护机构判断在该案例中，CentAR 没有对个人信息进行处理，因而也无需获取个人的授权同意。

(二) 隐私计算应用的常见误区

由于数据安全保护义务与数据处理使用的具体规则仍有待进一步明确，隐私计算的应用仍存在合规边界不清晰的问题，在实际应用中也存在一些误区。正确认识技术是发挥其最大使用价值的必要前提，也是避免滥用数据、规避合规风险的应有之义。

一个典型的误区是“**使用隐私计算即可实现个人数据的匿名化**”。隐私计算通过使用基于信息混淆、统计学、密码学等的各类方法，将数据泄露的可能性大大降低，但由于技术的实现方式庞杂，虽然有效的保护了数据处理的过程，仍然需要对处理的结果进行评估，如其在某些场景下可反映出单个个体的某些特征，也无法满足匿名化“不可识别、不能复原”的要求，输出结果依然属于个人信息，需要满足个人信息保护的合规要求。

第二个误区是“**如果隐私计算的参与方未获得其他方的原始数据，即无需获得个人的授权同意**”。由于授权同意属于数据处理的合法性基础之一，而隐私计算属于对数据进行处理、使用的一种技术手段，在流程和逻辑上需要依赖于合规基础的存在。因此，当参与方选用授权同意这一合规基础时，使用隐私计算处理数据这一目的或方式本身

需要被囊括在授权同意的内容当中，而非可以豁免授权同意这一前置条件。用户依然享有知情同意和拒绝等权利，企业也需要自证其数据的实际处理控制在用户授权的范围内。

第三个误区是“**当隐私计算未对原始个人数据进行处理时，不属于处理个人数据**”。由于隐私计算本身并非匿名化的必然实现方式，即使未获取到其他参与方的原始个人数据、仅获取数据切片、模型梯度等数据，也因为存在客观上可逆的可能性而仍然属于对个人数据进行处理。例如在终端使用联邦学习对用户行为进行建模时，参与方需要在终端收集用户的出行、消费等数据，并将模型的梯度信息进行交换。由于梯度数据被还原为原始数据的可能性较高，梯度数据仍然属于 “个人信息”，仍然受到个人信息保护相关法律法规的规制。

总之，隐私计算技术有利于解决参与方间互不信任而又需要进行数据流通的现实需求，有助于应对个人信息保护中“最小必要”和“保护数据安全”的要求，但无法实现跳过用户知情同意的目的，对于是否达到保证匿名化效果，还需按实际情况进行评估。所以，隐私计算无法绝对豁免合规要求，需要参与方根据具体应用场景、技术方案、参与方的约定等判断合规风险点。本白皮书将会在第三章对各类法律与合规风险进行展开阐述。

第二章

参与主体及其法律关系

隐私计算的参与主体众多，承担的义务和职能各不相同。明确各方的角色及其在各环节的权利、义务和责任将有助于顺利推进项目的进行。

(一) 参与主体的定义和主要职能

按照参与方在隐私计算过程中承担的职能，可将参与方划分为数据提供方、技术提供方和结果使用方三类。为了对数据的使用进行监管或评估，参与方也可能会考虑引入独立的第三方机构。

数据提供方是负责提供模型训练数据或隐私计算实际运算数据的主体。数据提供方的义务主要包括从数据控制者处获得数据使用的授权，向其他参与方告知数据使用的方式，对数据源的质量、合规、可用性等承担责任。其他义务可能包括负责数据的本地存储，对数据进行预处理等等。

技术提供方是负责提供隐私计算所使用的平台设施、技术方案、管理方案的主体，可根据参与方所承担的具体职能被分为计算方、调度方、算法提供方和平台提供方等主体。其中**计算方**负责提供算力支持，依照约定的计算方法接受数据提供方的输入因子并进行计算，并

在计算结束后将输出因子发送给结果使用方；**调度方**负责配置计算任务，管理和协调其他参与方执行任务；**算法提供方**负责提供计算逻辑和算法参数。值得注意的是，当参与方对算法参数有保护要求时，可将算法参数视为机密数据，并视情况将该算法提供方视为数据提供方；**平台提供方**则为综合上述全部或部分职能的角色，在实践中有时也作为技术方案的总包方。

结果使用方是接收隐私计算模型产出成果的主体，在实践中通常需要依照参与方对结果使用目的、范围和权限等方面的约定对结果进行使用。

第三方机构通常包括认证机构、评估机构等主体，本身不直接使用数据也不直接提供与数据处理相关的服务，其职能包括参与方资质认证与准入审核、数据质量评估、算法安全性评估、存证信息审计等。

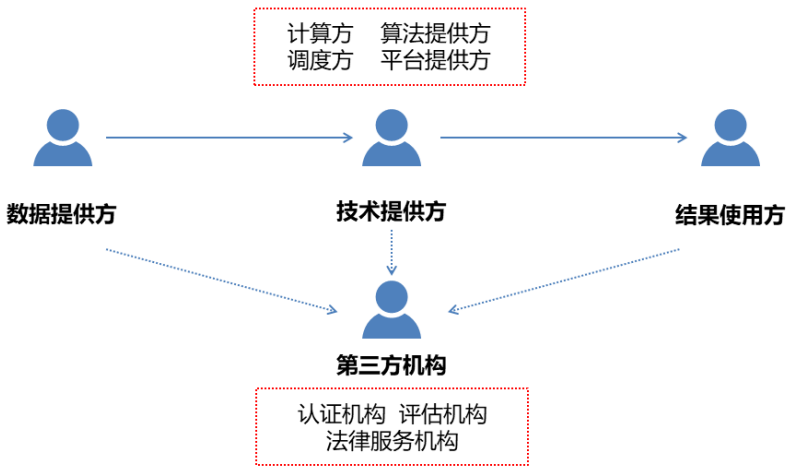

图 2 隐私计算参与方之间的关系

在实际应用中，数据提供方、技术提供方和结果使用方三者可能因参与方承担多重角色而存在重合。例如参与方 A 和参与方 B 共同进

行联合建模和结果预测，A 和 B 均提供部分用户数据，都需要获取预测结果，参与方 A 负责提供隐私计算平台，那么参与方 A 和 B 均是数据提供方和结果使用方，参与方 A 同时也是技术提供方。

(二) 参与方的法律定性

1.个人信息处理者

作为“个人信息处理者”，需要依据《中华人民共和国个人信息保护法》及其他相关法律法规的要求，遵循个人信息处理的规则，确保个人信息处理活动合法合规。构成个人信息处理者的关键判断依据在于是否能够**自主决定**个人信息的处理目的和处理方式。通常而言，当数据提供方和结果使用方可以对隐私计算过程中个人信息的处理独立施加影响时，两方均为个人信息处理者。

对技术提供方而言，如果仅提供算力、数据传输或存储等技术工具，则因其不拥有对个人信息的处理目的和方式的决定权而不属于个人信息处理者。

2.委托人与受托人

对技术提供方和第三方机构而言，其对于个人信息的处理往往需要遵循数据提供方或结果使用方的指示。因此，两类主体之间的关系属于《中华人民共和国个人信息保护法》第五十九条项下的“委托人”和“受托人”。作为受托人，技术提供方等主体应采取必要措施保障所处理的个人信息的安全，按照与参与方的约定处理个人信息，不得超出约定处理数据，处理结束后应当将个人信息返还个人信息处理者

或删除，不得超出法律许可和约定的期限保留数据。对于委托技术提供方进行个人信息处理的委托方，均需对技术提供方的选任、处理过程等承担相应的选任、监督责任。

第三章

隐私计算的法律和合规要点

在法律和监管层面，隐私计算技术乃至数据交易流通产业所涉及的合规红线仍不明确。在技术层面，要求隐私计算参与方完全避免技术固有的风险也不具有现实可能性。但我们仍建议参与方在分析技术产品和技术方案风险点的基础上，探索平衡合规、效率和精度要求的实践路径。

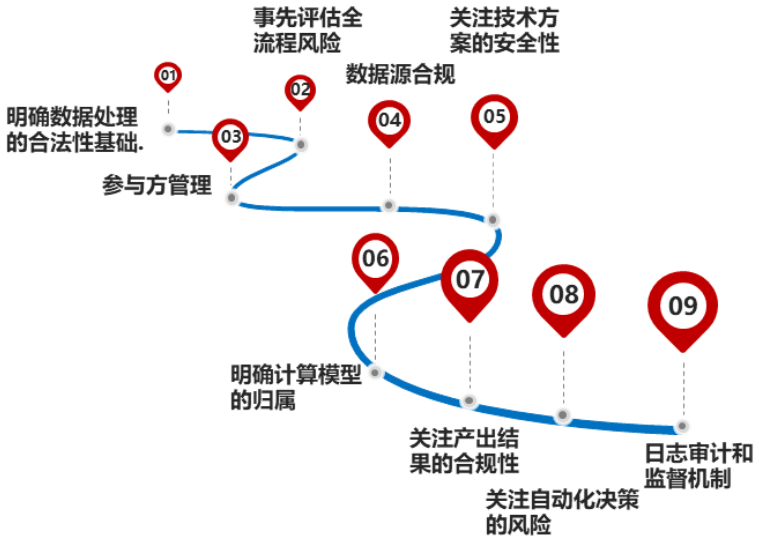

图 3 隐私计算法律与合规关注要点

(一) 明确数据处理的合法性基础

个人信息处理的一般原则要求数据处理者在收集、使用用户数据前获得有效的授权同意，明确数据使用的目的、方式、范围和规则等

内容。即使隐私计算的过程可能并不涉及到原始数据的流转，但由于隐私计算对数据的处理仅在特定条件下可达到匿名化的效果，数据处理的规则仍应得到严格的遵守。其中，特别要注意**用户授权链条的完整性**，即用户的授权应当覆盖全部的隐私计算参与方和隐私计算全部的操作行为。

除授权同意外，《个人信息保护法》还列举了其他几种数据处理的合法性基础，如：为订立、履行个人作为一方当事人的合同所必需；履行法定职责或义务；应对突发事件；为公共利益实施新闻报道和舆论监督或处理已经合法公开的信息等等。特别是在金融风控、政务、医疗数据处理等场景下，**隐私计算的参与方可以结合具体业务场景选择最为适合的数据处理合法性基础**。

(二) 事先评估全流程风险

根据我国《个人信息保护法》第五十五条的规定，当个人信息处理者有处理敏感个人信息，利用个人信息进行自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息等情形时，应当**事前进行个人信息保护影响评估，并对处理情况进行记录**。因此，参与方首先需要对隐私计算的具体场景是否涉及敏感个人信息、是否会对个人权益产生重大影响等事项进行事前的个人信息安全影响评估。评估的具体内容包括但不限于数据的处理目的和方式是否合法、正当和必要；对个人权益的影响及安全风险；保护措施是否合法、有效及与风险程度相适应等等。

第二，**参与方需要动态评估数据的使用场景是否始终符合用户的授权和参与方的约定**。根据《个人信息保护法》的规定，“处理个人信息应当具有明确、合理的目的，并与处理目的直接相关”。例如即使参与方接触的数据是数据模型、切片数据、加密数据等衍生数据，但对原始数据在本地服务器进行建模、对衍生数据进行计算或处理的行为本身同样应当被涵盖在用户授权的范围内。例如，在联合建模的数据处理环节，参与方需要对模型逻辑及各环节的数据需求进行梳理。若实际模型逻辑和需求与参与方加入时报备的不一致，则可能存在超范围使用数据的风险。

第三，**在数据输入模型后，技术提供方应根据数据的类型和安全级别等因素选择相适应的技术**。当对多个数据源提供的数据进行汇聚或融合计算时，还需对数据汇聚、融合后的安全级别进行动态的监控和评估。当输入的数据包含模型、参数等，也需要单独评估其逻辑的安全性和合理性。

第四，**隐私计算的参与方需要在保证安全模型完备性的前提下对每个节点的安全性进行考量**。在节点加入时，参与方应按照隐私计算平台的安全假设及相关规则，评估节点加入给隐私计算平台带来的影响。当涉及到数据提供方、算法提供方节点时，还需对输入平台的数据、算法等的安全性进行审查；另外，隐私计算平台也可通过节点加入的自动化审核和处理，减少人为干预带来的不可控风险。

第五，**数据处理的过程也应当注重数据安全保护**。参与方需要通过技术方案和协作机制确保隐私计算的过程数据、模型数据和最终计

算结果等数据的安全。参与方也需要避免计算模型的泄漏，防止攻击者通过逆向学习等方式获得原始数据。

第六，在数据存储方面，**技术提供方需要采用适当的密码算法确保数据和模型的存储安全**，及时清除内存中的数据，确保在处理敏感数据后无留存或隐通道传输，并依照参与方的约定对外部存储的数据进行不可还原的删除或匿名化处理。当应用隐私计算技术实现数据更大规模、更大范围的流动时，可能造成海量数据的汇聚，而由数据量提升带来的安全风险可能呈指数级增长，超出参与方可控的范围。为降低风险，参与方可选择数据的分布式存储，避免大量明文数据的物理汇聚。

(三) 参与方管理

由于隐私计算的参与方涉及多个主体，一方的合规风险可能会传导到其他参与方。再加上目前隐私计算的落地应用和具体规则也仍处于早期自发探索的阶段，参与方之间的法律关系也较为复杂，在正式开展合作前明确参与方的管理机制将有助于控制业务风险，顺利推进项目的开展。**参与方需要在应用隐私计算前通过协议的方式明确参与方之间的权利义务，构建完善的配合和监督机制**，以确保隐私计算任务的全流程得以有章可循，也避免在发生数据泄漏或其他侵害个人信息权益等事件时出现责任不清或互相推诿的情况。

具体而言，首先由于隐私计算的参与方可能是动态、多元的，设定参与方准入的标准将有助于避免与不适格的主体进行合作，降低整

体的风险。例如可以要求参与方具备较全面的数据安全管理能力，具备处理特定类型数据必要的资质等等。

第二，参与方需要**确认责任义务划分是否明确合理**，否则将可能会影响计算任务的顺利推进。例如需要对个人信息主体行使查询权、复制权、删除权等设计具体的分工配合机制，避免由于部分主体的推诿而使合规风险扩大至所有参与方。

第三，参与方应**明确对技术提供方的具体要求**，确保技术方案具有安全性和可靠性、数据结果具有可用性。此外，参与方也需要充分了解技术方案固有的风险，明确在出现数据泄露等风险时的应对机制和责任分担。

第四，参与方也需要**对合作方进行必要的风险提示**。在进行隐私计算产品和服务的推介时，建议厂商使客户和营销方对隐私计算有基本的认知，避免对其效果和功能进行夸张描述，避免其对隐私计算产生误解。例如，数据合作各方应当避免简单、直接将隐私计算作为“匿名化”的实现方案或替代方案。隐私计算在理想情况下将无法追溯到数据主体，这是隐私计算的一种优势，但不能与“匿名化”完全等同，也不能将使用隐私计算与彻底满足数据合规要求相混淆。

第五，**项目流程管理是合作方合规管理的重要组成部分**。在签订合作协议时，各参与方应制作项目计划等文件，明确立项、中期测试、验收、结项的各个时间节点和核验方式，以便及时发现问题并采取措施，加快响应速度和降低数据泄漏风险。在项目计划中，各参与方还可以对合法合规性、技术安全性、风险防控、投诉机制等内容予以细

化，并以此作为内部管理的标准，以便在合作中更好地将合规管理落实到业务流程中。

最后，参与方也可以考虑**引入第三方机构**。第三方机构能够提供的服务涵盖安全评估、合规评估、持续的安全审计等，能够为隐私计算项目提供更为客观、公正和专业的审核和论证，第三方机构的参与将有助于帮助参与方及时识别风险、落实安全保障义务、提供中立的审计鉴证等等。

(四) 数据源合规

隐私计算是一种多元数据的跨界合作，因此隐私计算的数据来源具有一定的复杂性，任何一个数据源受到污染均可能影响输出结果的质量。在《个人信息保护法》之下，参与方共同进行隐私计算很可能会构成共同处理个人信息。因此，数据源合规成为了牵一发而动全身的问题，我们建议在将数据投入计算之前，**数据合作各方应当各自核查及确认其数据来源的合规性，避免影响隐私计算的整体安全与合规**。

隐私计算本身不能解决数据来源的合规性问题，数据提供方需要根据数据的不同来源对数据的合规关注点进行梳理和确认。例如常见的数据来源包括直接数据源（例如移动终端、APP、小程序、互联网网站、物联网设备、营业厅等）；间接数据源（例如向提供方采购、与参与方共享的数据等）；公共场所采集（例如人脸识别、步态识别等个人身份识别采集等）。

对**直接数据源**而言，最主要的合规关键点在于获取个人信息主体

充分自主、清晰明确的授权同意。当存在获取授权的方式不合规、用户隐私协议不规范等问题时，则可能为数据的后续使用和其他参与方带来合规隐患；此外，根据《数据安全法》、《关键基础设施安全保护条例》等法律法规的要求，对于可能对国家、社会、民生造成严重影响的数据，应确保该数据标的满足风险评估、备份、加密和境内存储等安全保障义务，或在主管机构提供的平台进行监管下的“场内”融合和共享。

对**间接数据源**而言，应要求数据提供方说明个人信息的来源，了解已获得的授权同意范围并尽可能对其合法性、真实性进行确认；当隐私计算所需进行的个人信息处理活动超出授权同意范围的，应再次征得个人信息主体的明示同意等等。

此外，参与方也需要关注重要数据、未成年人数据、公共场所采集数据等特殊类型数据的合规要求。例如对公共场所获取的数据而言，采集数据应当为维护公共安全所必需，并设置显著的提示标识，或取得个人单独的授权同意等等。参与方也需要特别注意特殊类型敏感数据的处理收集，如：民族或者种族背景、政治立场、宗教哲学信仰、基因数据、旨在识别特定自然人的生物识别数据、与自然人的身体健康状态相关的数据等。

(五) 关注技术方案的安全性

参与方需要对隐私计算技术方案的建模预处理及运算过程进行充分的安全性评估。以联邦学习建模的场景为例，其主要流程包括样

本匹配、特征工程、模型算法等。在样本匹配中存在大量的数据交换，应当保证各方均不能通过过程数据反推出除共有样本外的其他原始数据；在特征工程中，在对参与方联合建模所使用的特征变量进行处理时，应使用合适的加密方式处理各方的特征信息；在联合建模阶段，参与方应确保各方提供的数据只在本地进行模型参数计算，所有用于交互的数据均只能是各自运算结果的中间参数，如梯度值、损失函数值等。另外，也应采用适当的措施保护中间参数在传输与融合计算中的安全，尽可能降低数据泄露和反推出原始数据的风险。

此外，**参与方需要对隐私计算平台中涉及敏感数据处理的关键代码进行审计**。隐私计算一般基于特定算法使用数据，虽然可以通过密码学技术等方式对数据进行保护，但由于应用算法、模型的日趋复杂，仍可能存在一定的安全隐患，例如多次重复使用相同输入数据生成特定关系的结果可能会导致原始数据泄漏。因此，相关参与方需要对算法（即数据的使用方式和目的）进行安全性和合理性评估，确认数据泄露的风险可以被控制在可接受的范围内。

(六) 明确计算模型的归属

计算模型一般是指由特定训练数据使用特定的算法和参数训练出来的模型算法，其呈现形式可以是模型的源代码、模型结构或参数。由于隐私计算尚处于前期探索阶段，各方关注的重点多放在模型的效果层面，对于计算模型的归属和使用权限分配方面的研究仍较为薄弱。参与方如未能在合作开始前达成一致意见，则很可能在计算模型应用

规模扩大后因后续争议影响计算模型的使用。

在模型的知识产权方面，参与方需要约定开发后代码的归属，例如可以赋予结果使用方相应的知识产权，在纵向联邦学习中约定各参与方对部分模型享有知识产权等等。**在模型的使用权限方面**，参与方需要约定是否可以基于计算模型的源代码进行定制化开发等细节。拥有模型知识产权的主体也可选择不同形式的使用权许可，例如专有许可使用（即仅允许模型购买方使用该模型）；排他使用许可（即仅允许本方以及模型购买方使用该模型）；普通使用许可（允许本方以及模型购买方使用该模型，并且可以继续许可其他方使用该模型）等等。

(七) 关注产出结果的合规性

在输出最终计算结果时，各参与方需要尽可能控制输出结果带来的泄露隐私的风险。例如在医疗机构就某种疾病进行联合建模的场景，如果在输出预测结果的同时泄露了患者的 ID，则有可能泄露患者本身患有某种疾病的敏感信息。因此医疗机构可能需要通过隐私集合求交集或隐私信息检索等方式在预测疾病风险的同时不泄露患者的 ID，从而实现输出结果阶段的隐私保护。

在结果的使用阶段，**参与方应对输出模型和结果数据的使用进行明确的约定**，要求结果使用方依照参与方约定的使用目的、范围和时限等要求使用数据和模型。尽管在实践中参与方很难对结果使用方的数据使用行为进行监督和约束，我们仍建议参与方通过合同切分义务和责任、明确违约责任、采用限制 IP 技术等方式控制结果的使用，

进而减轻结果使用方可能为其他参与方带来的合规隐患。

另外，在实践中关于输入数据的风险是否会传导到输出结果的问题也有诸多争议。例如当部分结果接收方本身没有参与联合建模，最终输出的统计数据等结果无法识别到原始信息，基本满足匿名化的要求，但输入的原始数据本身存在权利瑕疵。在这种情况下，原始数据的风险是否会影响结果方使用输出结果的权利，仍然有待立法和实践的进一步探讨。

(八) 关注自动化决策的风险

当隐私计算的模型的使用目的是信息推送、商业营销时，参与方也需要关注自动化决策的合规风险。例如当模型可被用于精准推荐时，隐私计算的参与方须根据具体场景的要求考虑决策的透明度披露和结果的公平公正，不得导致会对个人实行不合理的差别待遇。

此外，当结果使用方需要通过自动化决策向个人进行信息推送、商业营销时，也应为用户提供不针对个人特征的选项或向个人提供便捷的拒绝方式。

(九) 日志审计和监督机制

由于隐私计算对原始数据进行了统计学、密码学等方式的处理转换，技术本身具有一定的复杂性和黑盒属性。另外，隐私计算涉及到硬件、软件、网络安全等诸多实现细节，技术人员和业务人员的操作也可能会影响技术方案的安全性。在极端情况下，数据交易的参与方

甚至可能打着隐私计算的幌子进行非法数据交易。因此，**为提升参与方和监管机构对技术的信赖，参与方需要提供有效的存证和监督机制，并考虑构建隐私计算技术应用效果的评估机制。**

针对隐私计算的输出结果，目前实践中主要以安全验收作为合规的标准。参与方可通过电子合约的形式确定各方权利义务并建立针对过程数据和计算结果的安全合规确认和存证机制。中间结果的日志留存认证主要指通过日志或其他形式保留计算过程，对数据的获取、传输、处理等过程证据进行保存，以满足内外部监管要求，避免发生安全事件时的举证困难。最终计算结果的合规认证则是指在输出计算结果时进行再次核查以确保隐私计算的结果不可逆，符合主体授权或履行合同的范围，不会导致泄漏风险等。

第四章

隐私计算的应用实例效果评估

隐私计算在平衡数据流通过程中的监管合规和安全保护中发挥的作用得到越来越多行业和机构的关注和应用，政务、金融、营销等行业的隐私计算应用逐渐落地开花。

(一) 广告营销场景

广告营销是隐私计算落地的一大热门场景，隐私计算参与方在现有成熟的广告程序化交易基础上，将隐私计算技术运用于联合建模和数据流转的流程中，最终实现降低合规风险和提升广告投放效果的目的。该业务的数据流转如图 4 所示：

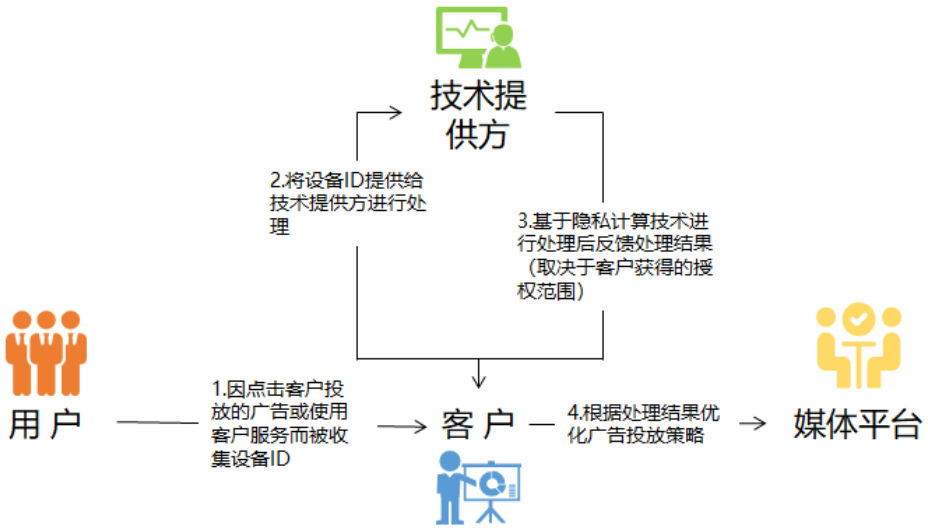

图 4 广告营销场景隐私计算数据流转示意图

“客户”即结果使用方，是上述流程的关键合规节点。结果使用方一方面从用户处直接获取个人信息，或从其他数据处理者处间接获取个人信息；另一方面也会将用户 ID 等部分数据提供给技术提供方等主体，委托其对数据进行进一步的加工处理。对获取数据这一环节而言，结果使用方需要审查确认隐私计算模型使用的数据来源是否合规，隐私计算对数据的处理过程和最终的处理结果是否在用户的授权范围内，最终处理结果是否不精准关联个人、不涉及用户权益等；对后续数据流转的环节而言，结果使用方需要对技术提供方提出基本的合规要求，除了要求技术提供方给出服务过程中的安全承诺外（例如不会未经授权的查看、复制或转移数据），在服务结束后还需要求技术提供方删除留存的数据。

对技术提供方而言，其实际上是依照结果接收方的要求处理数据，虽然本身无权决定和控制数据的来源和处理的方式，但也应在接受委托前，就数据处理需求是否合规进行基本的审查，以免因结果接收方的过错导致承担连带责任。例如，当结果接收方提供了一批已加密的设备 ID，希望运用隐私计算技术对设备 ID 进行处理，并最终获得针对单个设备 ID 的标签。由于该场景涉及个人信息的处理，技术提供方需要对数据来源及授权范围进行书面审查，获得结果接收方关于其已获得用户画像授权的合规承诺，否则技术提供方将可能承担为结果接收方补足个人信息的风险。

(二) 个人融资风控场景

金融电信数据融合应用于反欺诈是金融风控的主要场景之一，在金融机构数据和运营商数据均包含用户个人隐私、无法出域的情况下，采用多方安全计算技术能够对双侧数据进行密态计算，在保护个人隐私的同时利用数据的价值。

为了进一步打击金融犯罪，在多方安全计算的技术方案中融合图计算技术可以进一步提升对犯罪团伙等异常用户的识别效率。在银行及运营商侧通过主流图数据库以拓扑结构图数据的形式保存用户的金融交易行为和通讯浏览行为等信息，在双方本地加载用户关系图数据和部署节点资源，在数据的源头减少了隐私泄露的风险；在此基础上，平台对银行及运营商的联合关系图谱进行刻画，在无法获知对方原始图数据的情况下进行联合图数据处理与计算。

从参与方的角度而言，银行和运营商作为数据提供方需在获取用户授权的前提下以最小必要原则采集用户数据，并对图库数据源的质量、合规及可用性等承担责任；技术提供方仅提供图处理、图计算及计算结果查询服务，全过程不接触原始隐私数据；银行作为结果使用方需要依照对结果使用目的、范围和权限等方面的约定对平台查询结果进行使用。在数据交换的过程中，银行及运营商均需保证交换的数据经过去标识化或匿名化处理，且双方均无法通过中间结果等反推共有样本外的其他原始数据。

在技术方案的设计方面，如图 5 所示，多方安全图计算平台包含基础层、计算层和应用层：其中基础层基于主流图数据库加载用户的

银行账户转账记录、运营商通话时长、通话频次等拓扑结构图数据；计算层根据基础层返回的数据提取结果进行图处理和安全图计算；应用层根据计算层返回的计算结果向用户提供图谱导入和密态图谱查询服务。

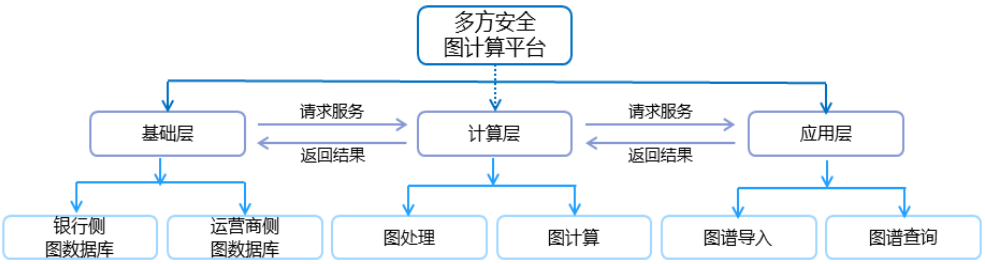

图 5 多方安全图计算平台技术架构

基于银行及运营商各自的图数据，多方安全图计算技术能够实现欺诈黑名单染色、查询功能和双向图融合功能。在黑名单染色及查询过程中，银行侧对用户黑名单中的手机号进行哈希，哈希方法无法逆推得到用户手机号明文，具有数据去标识化的效果；银行侧对用户黑名单属性值进行半同态加密得到密态值并发送至运营商，密态值也无法逆推得到属性值明文。在这个过程中，同态加密技术保证先计算后解密的效果等同于先解密后计算，因而可以减少计算过程中泄露明文信息的风险，能够保护银行的黑名单信息。

在运营商侧，根据哈希后的手机号找到本侧图网络中对应的中心节点（即运营商用户），并将中心节点与关联节点以连线的方式刻画出本侧的用户关系。在运营商对来自银行的用户黑名单属性密态值进行密态计算后可得到关联节点的权重值，并在本侧对相应用户进行染色处理。银行侧在进行运营商黑名单查询时，可以通过输入哈希后的

手机号，由运营商侧返回节点的黑名单密态值，再由银行侧解密得到用户黑名单属性，从而辅助银行风控人员对用户欺诈行为进行预判。

(三) 小微企业信贷风控场景

先进的个人信用风险预测模型需要大量更全面、更真实的数据来提升算法性能，但数据的高隐私性和各机构间互不信任的现状都导致单家金融机构无法利用大量数据进行模型训练。具体而言，银行主要面临两方面的挑战。一是数据采集范围局限，可用于线上审批模型构建及策略设计的基础数据主要来源于人行的征信数据，获取及应用来自互联网生态的数据存在较多客观限制。二是隐私保护的要求，即如何在确保数据隐私的前提下，实现与合作方的数据融合和挖掘。

为了解决以上挑战，基于多方安全计算技术的平台可以在保护用户隐私和数据安全的前提下，引入外部数据增强模型的风控效果，以便对小微企业进行更准确的授信判断。该平台的技术架构如图 6 所示：

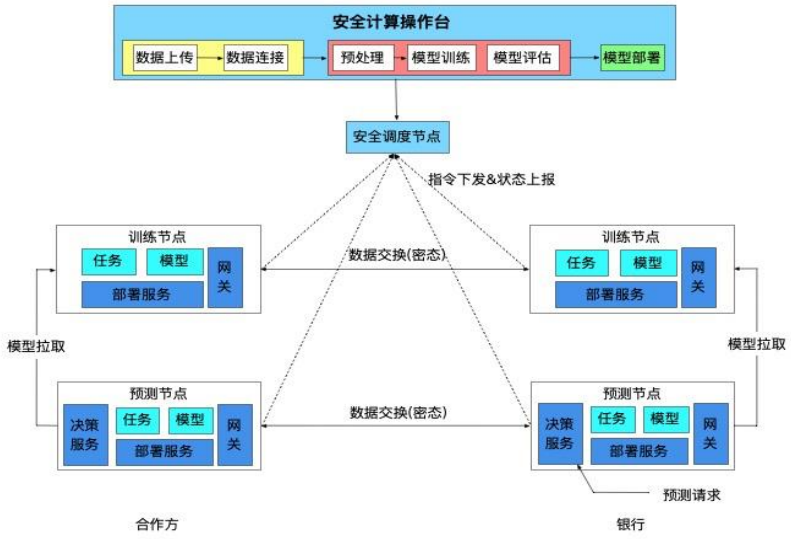

图 6：多方安全计算训练流程

在执行隐私计算任务之前，隐私计算的参与方约定的建模的规则，用于明确数据的使用目的、范围和时限等要求。数据提供方需要将训练数据样本上传至各自的数据存储服务器，之后建模人员按照约定的规则在多方安全计算平台通过可视化页面构建数据融合、特征工程、模型训练、模型评估等工作流。工作流以任务形式下发到协调器，后者将任务调度到对应节点的训练引擎，由训练引擎根据任务描述读取本地样本数据，并使用多方安全计算协议与对端协同完成一次训练任务。在训练任务完成后，训练引擎将模型文件保存至各自的模型存储服务。

多方安全计算技术运用了秘密分享、同态加密等密码学技术，将原始数据转换成密态数据进行交互，完成了数据的建模，整个过程中不会透露原始数据，各参与方均无法通过中间结果等反推出其他方的原始数据。不仅多方安全计算技术有助于保证技术的安全实现，而且可在整个隐私计算过程中对数据输入过程、结果输出过程等关键环节进行存证，对计算过程中的相关结果和信息进行记录。

(四) 金融穿透式监管场景

我国传统的金融监管以分业分段式监管为主，不同金融业态和从业主体由不同部门监管，监管数据统计均由金融机构定期报送，各业态间存在统计标准不一、信息分散、数据共享较难等困境。资金流水数据通常由商业银行掌握，且属于个人敏感信息，难以直接将原始数据分享给监管平台。此外，如果平台只是在系统数据库中专门设置一

套用于监管报送的数据，仅通过监管系统设置的内部勾稽关系验证，那么监管系统将很难在缺少资金流穿透等其他辅助手段的情况下发现此类违规行为，账外交易的风险也同样难以被有效监测。

针对资金流穿透监测的数据的特点，从目标需求属性来看，资金流水核验需求比较简单，业务核验本身的实时性要求不高，设置为T+1日核对T日发生的资金交易数据即可满足需求。从数据属性来看，具体包括了各机构上报的业务交易信息和银行上报的资金流水信息，如业务类型、交易金额、交易当事人身份证号码或组织机构代码等，数据量比较大，更新较为频繁。从法律合规属性来看，交易金额、当事人身份证号码等属于C2类个人金融信息，主管部门对其保密性要求较高。由于穿透监管所涉及的数据体量较大，对结果准确性也有较高的要求，因此综合考虑来看比较适用于运用多方安全计算进行资金流水核验，对上报交易要素与交易行为的一致性进行审核。

该平台的逻辑框架具体如图7所示，从业机构的业务数据和资金交易银行的业务交易流水数据均经数据密文接入模块处理后输入监管平台，随后由平台融合计算出业务的资金流水对账结果，并以密文形式发送至监管方，最后由监管方解密进行对账审查。此方案实现了资金流水数据的安全共享应用，且免除了传统模式下的现场监管实施成本，同时帮助监管当局增强交叉性金融风险监测水平，助力金融行业健康发展。

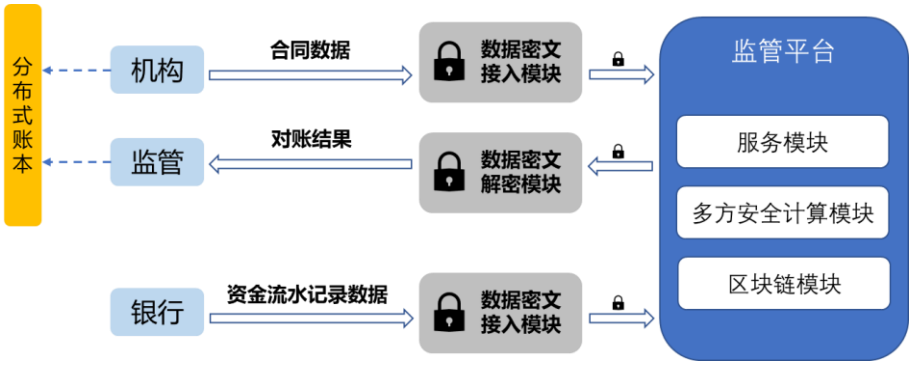

图 7 穿透式监管系统整体框架图

此外，平台还可通过扩展对接人工智能、区块链技术，实现风险自动化预警，以及全流程操作和存证的防篡改、抗抵赖和可溯源等。通过多方安全计算的应用，有助于减少非现场监管模式下获取信息失真的风险，提升金融监管的专业性、统一性和穿透性，降低现场监管实施成本，增强跨行业、跨市场交叉性金融风险防范能力，有力促进金融行业健康、稳定、高效发展。

(五) 人脸识别场景

随着人脸识别在各行业的广泛应用，人脸识别所产生的数据在传输、存储、使用等环节中均存在个人信息泄露、滥用、超范围共享等安全风险。隐私计算技术有助于防止人脸等敏感信息的泄露，在结合数据溯源、区块链等技术对数据的使用进行存证后，有利于有效地保障数据安全。

基于秘密分享机制实现的多方安全计算协议可以构建一个安全的人脸识别平台。一方面平台可以提升人脸识别数据在注册和存储中的安全性。平台由多个计算节点组成，遵从随机密钥分发协议和计算合约执行人脸识别，即使某个计算节点被恶意攻击，依然能够保证人

脸识别数据的安全；另一方面，平台可以应对人脸识别数据在比对中的安全问题。平台利用秘密分享机制实现人脸识别数据的密文注册和比对，可以有效的加强人脸识别中的隐私保护水平。在整个人脸识别的过程中，计算出的密文识别结果会直接发送到数据使用方解密使用，平台的技术提供方无法直接获取被查用户的人脸特征值，从而在保证个人信息不会泄露给第三方的同时，实现了人脸识别数据的定向应用。具体方案如图 8 所示：

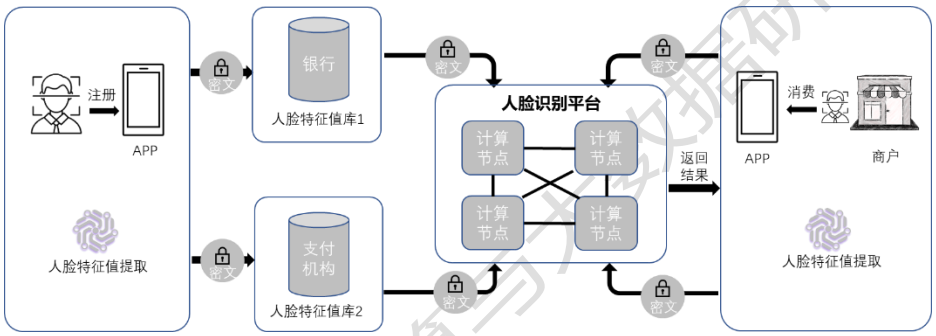

图 8：基于秘密分享的人脸识别

例如，用户在个人终端开通人脸识别支付服务时，终端设备内嵌的算法提取人脸特征值，并将 ID 与人脸特征值发送到本地加密模块。加密模块使用秘密分享的方法，对用户 ID 及人脸特征值进行随机的加密分片，并通过安全通道或专线分别将分片的密文数据传输到银行、支付机构等不同实体的人脸特征库中进行分离存储。

当用户通过 APP 进行支付操作时，需要通过人脸识别核实身份信息，从而触发人脸识别数据比对。终端设备利用其采集的人脸图片提取人脸特征值，内嵌加密模块使用秘密分享的方法对人脸特征值进行加密分片，分别发送到平台的不同计算节点缓存。在管理模块的任务调度下，将从各机构人脸特征值库中提取的密文数据分片与缓存的密

文数据分片在全密文环境下进行比对，并将密文人脸识别结果分片返回到终端。在解密模块进行拼装解密后，APP 根据解密后得到的身份识别结果，继续完成支付业务流程。在全流程中，除了数据主体外的其他各方，均没有得到完整的人脸特征值，从而保证了整个人脸识别过程中的隐私安全，同时也减小了银行、支付机构等所承担的安全风险。

第五章

隐私计算合规发展的展望

严格的合规要求一方面是隐私计算发展的巨大压力，另一方面也同时是隐私计算市场需求的重要来源。在隐私计算产业发展的初期，建立与行业参与者、监管机构的良性互动将帮助隐私计算技术不断修正发展的方向，不断拓宽应用的场景，形成稳健有序的整体发展态势。

(一) 鼓励创新，留足空间

在国家保障数据安全和促进数据利用并重的大原则下，隐私计算作为正处于高速发展期的新兴技术，有助于提升数据流通的合规性，降低企业数据合规的成本。当然，行业参与方也应清晰地认知到，由于技术发展水平固有的局限性，隐私计算无法彻底解决各应用场景的合规问题。从立法和监管的角度而言，我国可参考域外隐私保护法规落地的社会效果，综合欧盟保护个人基本权利和美国保护自由市场竞争秩序的两种路径，在立法和执法实践的大方向上寻求效率提升和合规安全间的平衡。由此，鼓励技术创新来解决合规问题得以成为行业的共识，隐私计算技术和产业可获得更大的发展空间，未来也可为创造高效安全的数据要素交易环境提供更为坚实的技术支撑。

(二) 以点带面，逐步深入

新兴技术的发展普及需要技术迭代和产业健康良性的竞争，针对技术监管的逐步完善也有赖于监管机构、产业界和学术界的共同参与。在隐私计算发展的初期，金融风控、数字营销等较为成熟的应用场景和试点沙盒可为行业积累宝贵的经验。在此基础上，隐私计算在各行各业的落地实践有助于与时俱进地调整监管的重点和方向，为数据分类分级、数据交易等制度的推进和完善发挥积极的作用。

(三) 多方参与，各尽其能

隐私计算是一门多学科跨领域的综合技术体系，有限的监管监督资源在面对多样的技术方案和丰富的应用场景时很难做到面面俱到。因此隐私计算需要在监管机构政策引导的前提下，充分利用好隐私计算服务方的技术优势，充分调动行业参与方的力量。在逐步建立行业共识的过程中，行业自律组织和标准化组织也需要积极发挥作用，一方面将技术方案和合规要求标准化，另一方面促进行业优秀实践的沉淀和推广。

与此同时，经国家认证授权的第三方评估机构也可通过出具等级评定和咨询等方式，根据业务需求对不同行业和场景下隐私计算的过程及结果合规进行监督和鉴证。总体而言，监管机构、行业自律组织和第三方评估机构等多方参与的合规监管体系，有助于隐私计算技术的迭代普及，推动达成国内国际双循环、加快培育数据要素市场的总体目标。

(四) 层级分明，分类监管

在《网络安全法》《数据安全法》和《个人信息保护法》的统摄下，地方法规、部门规章、行业标准、自律公约等将逐渐形成一整套自上而下、逐渐深入的规范体系。对隐私计算技术创新和合规落地而言，可以针对不同风险场景和行业应用从宏观政策导向到具体实施办法中寻求更加明确的合规指引。由此参与主体能更明确地了解其在隐私计算项目中的合规义务，监管规范的可落地性也可得到有效加强。与此同时，借助行业标准和第三方机构的合规等级认证，隐私计算的行业优秀实践可得到标准化和低成本的推广，最终多层次、分类别的隐私计算合规监管，可以促使各参与方间的利益分配达到动态平衡，保障隐私计算的高效稳健发展。