隐私计算技术在开放银行数据合规中的应用与面临的挑战

魏博言　强　锋　安文森

摘要：开放银行是依托数据流通技术而兴起并得以迅速发展的银行业新模式，然而银行数据的流通不仅关系着个体隐私安全，更关系着国家金融安全和信息安全。隐私计算技术作为一种隐私保护技术，能够在一定程度上解决开放银行数据共享过程中的痛点。本文在分析开放银行面临的数据合规要求的基础上，探讨了隐私计算技术对于满足开放银行的隐私保护要求具有的价值和优势，并对典型应用场景进行展望，最后指出隐私计算技术在开放银行数据合规应用中面临的挑战。

关键词：隐私计算；开放银行；数据合规；应用；挑战

一、引言

数据逐渐成为数字经济的核心生产要素，数据要素的重要性日益受到关注。2020 年 3 月 30 日中共中央、国务院在《关于构建更加完善的要素市场化配置体制机制的意见》中再次将数据作为与土地、劳动力、资本、技术并列的生产要素，并指出要加快培育数据要素市场、提升社会数据资源价值、加强数据资源整合和安全保护。

数据要素价值的利用和实现离不开数据的开放、可信流通和安全共享。然而，数据的可复制性和极低的边际成本意味着一旦发生数据安全事故，个人隐私将受到严重侵害，银行的数据资产价值将极大缩水，数据掌控能力也会下降，国家金融安全和信息安全也将面临威胁。因此，数据安全不仅是监管机构的监管重点，也是关系到银行客户、银行

作者简介：魏博言、强锋，中国工商银行软件开发中心；安文森，北京市路盛律师事务所。

本身以及国家利益的关键问题。近年来，国家相继出台了《网络安全法》《数据安全法》以及《个人信息保护法》，中国人民银行发布了《商业银行应用程序接口安全管理规范》和《个人金融信息保护技术规范》等。上述法律和行业标准的出台表明金融数据安全合规需要满足更高的要求。

开放银行通过 API（应用程序接口）与 TSP（第三方服务提供商）等技术将银行服务与产品直接嵌入合作平台，实现了银行与第三方之间的数据信息共享与融合。开放银行作为一种依托数据流通技术而兴起和迅速发展的银行业新模式，其数据合规面临着越来越多的挑战。随着中国开放银行的实践不断深入，开放银行中数据要素的使用和隐私数据的保护两者之间的恰当平衡具有重要的现实意义。

在这一背景下，面向隐私保护的隐私计算技术受到了银行业的极大关注。2021 年 5 月 26 日，国家发展改革委、中央网信办、工业和信息化部、国家能源局联合印发《全国一体化大数据中心协同创新体系算力枢纽实施方案》，明确提出利用多方安全计算、隐私计算等技术模式，构建数据可信流通环境，提高数据流通效率。隐私计算正在数据合规强监管和数据应用强需求的驱动下成为激发开放银行业务生态势能的重要手段。

二、开放银行数据合规相关要求

（一）法律对开放银行数据合规的总要求

开放银行的数据合规总要求，是指法律规范要求数据处理者在数据全生命周期的各阶段处理数据时均应遵循的准则，也是监管机构制定管理制度以及开放银行进行具体数据处理行为的依据。根据《民法典》《网络安全法》《数据安全法》《个人信息保护法》等，开放银行数据处理者需遵循合法正当、公开明示、知情同意、最小够用、数据安全与可问责性、准确完整等原则。

1. 合法正当原则

《民法典》《网络安全法》《数据安全法》和《个人信息保护法》等均指出处理个人信息应当遵循合法正当原则。例如，《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。《个人信息保护法》第五条规定，处理个人信息应当遵循合法、正当、必要和诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

2. 公开明示原则

《个人信息保护法》第七条规定，处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知法定事项，通过制定个人信息处理规则的方式告知法定事项的，处理规则应当公开，并且便于查阅和保存。该项原则保证了数据主体对个人信息处理的知情权。

3. 知情同意原则

知情同意是法律确立的个人信息保护核心规则，是保障个人对其个人信息处理知情权和决定权的重要手段。除有法律特殊规定，处理个人信息应当取得个人的同意，并且该同意应当由个人在充分知情的前提下自愿、明确作出；而且，特别要求个人信息处理者在处理敏感个人信息、向他人提供或公开个人信息、跨境转移个人信息等环节应取得个人的单独同意。数据处理者需要以容易理解的语言对数据处理的范围、过程和目的等内容进行明确告知，告知后以合法的方式征得数据主体同意，不得采用捆绑性同意等方式。

4. 目的限定原则

《个人信息保护法》第六条规定，处理个人信息应当具有明确、合理的目的，并应当与处理目的

直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。该原则要求在处理个人信息时，不仅数据处理的目的恰当，而且在满足处理目的的前提下，还应以最低频次和最短时间处理的方式进行。

5. 安全保障原则

《个人信息保护法》第九条规定，个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。这要求数据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采取相应的保护措施，例如，制定管理制度和操作规程，采取安全技术措施，定期进行安全教育和培训，制定并组织实施个人信息安全事件应急预案等。

6. 准确完整原则

《个人信息保护法》第八条规定，处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。数据主体有权要求数据处理者更正、补充或删除有关信息。

（二）金融行业标准对开放银行数据合规应用的特别要求

开放银行是一种银行向第三方开放数据和服务的新模式，因此，除了需要遵守数据合规的总要求之外，还需要遵循金融行业特有的数据应用标准。中国人民银行在 2021 年出台的《金融业数据能力建设指引》，明确了金融业数据能力建设应遵循五大原则，即用户授权、安全合规、分类施策、最小够用和可用不可见。

数据授权要求明确告知用户数据采集和使用的目的、方式及范围，确保用户充分知情，获取用户自愿授权后方可采集使用，严格保障用户知情权和自主选择权。

在数据获取和使用方面要求确保数据专事专用、最小够用，杜绝过度采集、误用、滥用数据，切实保障数据主体的数据所有权和使用权。

在数据共享方面，要求建立规范的数据共享机制，在保障原始数据可用不可见的前提下，规范开展数据共享与融合应用，保证跨行业、跨机构的数据使用合规、范围可控，有效保护数据隐私安全，确保数据所有权不因共享应用而发生让渡。

在数据治理方面，要求分类施策。综合考量国家安全、公众权益、个人隐私和企业合法利益等因素，根据保密性、完整性、可用性等属性对数据进行分级分类管理。对不同级别的数据进行分类，采取差异化控制措施，实现数据精细化管理。

安全合规即遵循国家法律法规、管理制度，严控访问权限，严防数据泄露、篡改、损毁与不当使用，依法依规保护数据主体隐私权不受侵害。

三、隐私计算技术在开放银行数据合规中的应用

根据大数据联合国全球工作组（Big Data UN Global Working Group）的定义，隐私计算是在处理和分析计算数据的过程中能保持数据不透明、不泄露、无法被计算方以及其他非授权方获取的一类技术的范畴和集合。隐私计算本质上是一种在保护数据隐私的前提下解决数据价值流通、实现数据融合、体现数据价值的机器学习和联合分析的方法。隐私计算的理念包括：数据可用不可见，数据不动模型动；数据可用不可见，数据可控可计量；共享数据价值，不共享数据。

目前隐私计算技术包括基于协议的多方安全计算、基于密码学的联邦学习和基于硬件的可信执行环境三大技术分支，实现了在数据隐私保护基础上数据价值的流通。上述三大主流隐私计算技术的实现，依赖于更加底层的密码技术或安全协议，分别

是差分隐私、不经意传输协议、混淆电路、秘密分享、同态加密、零知识证明等。

通过对差分隐私、同态加密等隐私计算底层实现技术的定义、适用场景等进行分析和对比，不难发现，这些技术在保护个体隐私、保障数据安全方面具有巨大的优势，详见表 1。

上述隐私计算技术的特性，可以使得开放银行在数据共享的过程中，满足目的限定、安全保障、最小够用、安全合规、可用不可见的原则。因此，基于隐私计算技术的开放银行隐私保护解决方案，可以依托差分隐私、同态加密等底层技术来实现。

四、应用场景展望

开放银行在满足了知情同意、公开明示、分类施策、用户授权等原则的基础上，可以通过隐私计算技术进一步实现安全合规的数据共享以及数据要素价值释放，激发银行的新业态发展，助推银行数字化转型。根据隐私计算技术的特征，未来隐私计算技术在开放银行发展中或可有如下应用场景：

（一）基于不经意传输协议的信用卡额度预测场景

移动支付的普及使得第三方支付公司积累了大量的用户消费记录，这些数据很大程度上可以反映用户的消费习惯、消费水平。银行在面对个人信用卡用户申请时，如果能够通过这些数据对用户的偿还能力和资金水平进行判断，将会大大提高授信额度决策的合理性，进而提高银行的风控水平。基于隐私计算技术的开放银行接口可以满足支付公司和银行方数据的合规共享。在用户对数据处理方式充分知情同意并进行相应授权后，支付软件可以将用户的明细数据抽象成某种规则类特征。银行可通过开放银行接口基于不经意传输协议与支付软件交互，通过规则判断的方式获得支付软件侧特征所反映出来的用户信息（例如月均消费额度是否大于 5000 元等）。基于不经意传输协议的特性，支付软件侧不会得知银行向支付软件查询的特征信息，保护了银行的隐私；银行侧仅能得到查询结果，而不会得到除结果之外的任何信息，也保护了支付软件侧的数据，并且用户的明细数据不会被直接传输而导致信息泄露。上述方案充分满足了最小可用原则和数据可用不可见原则，为用户和银行的隐私都

表 1　隐私计算技术分类及适用场景

技术分类	定义	适用场景	优势
差分隐私	在提供统计数据查询时，通过引入随机项，最大化统计数据查询的准确性，同时最大限度减少识别其单一个体记录的机会。	统计数据发布、个人数据采集	维持群体数据统计特征的可用性；保护个体隐私
不经意传输	通信双方都以一种选择模糊化的方式传送消息，消息发送者无法得知接收者收到了哪条信息，同时消息接收者也无法知道其他不相关的消息。	匿踪传输、隐私集合求交、联邦学习	保护个体隐私
混淆电路	核心技术是将两方参与的安全计算函数编译成布尔电路的形式，又将真值表加密打乱，从而实现电路的正常输出而又不泄露参与计算的双方私有信息。	联合数据分析、数据安全查询、数据可信交换	保护数据安全
秘密分享	将秘密以适当的方式拆分，拆分后的每一份额由不同的参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息。	联合数据分析、数据安全查询、数据可信交换	保护数据安全
同态加密	允许用户直接对密文进行特定的代数运算，得到的数据仍是加密的结果，该结果与对明文进行同样代数运算再将结果加密一样。	隐私保护云计算、联邦学习	保护数据安全；保护个体隐私
零知识证明	证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。	匿名身份认证	保护个体隐私

提供了保障。

（二）基于差分隐私技术的开放银行智能选址服务

目前，越来越多的银行进行了生活类开放银行接口的开发，例如银行支付软件中提供的餐厅选择、电影票购买等功能。用户使用此类功能时，支付软件会对用户的地理位置信息进行收集，以推荐就近的就餐场所或电影院。在这个过程中，可以基于差分隐私技术对用户地理位置加入扰动，再通过接口传输至银行方，保护用户的个人隐私。在银行收集到大量经过差分隐私扰动后的用户地理位置数据后，可以将其与银行所拥有的大量用户消费数据相结合进行统计分析，并根据分析结果，通过开放银行服务，向餐饮商户提供门店智能选址的数据产品。在提供上述数据产品时，可再次使用差分隐私技术对用户信息进行去标识化处理，使用户个人的隐私数据得到双重安全保障，进一步满足开放银行数据共享的安全合规要求。

（三）基于秘密分享技术的联合统计场景

银行在对小微企业进行贷款资质审核时，为了更好地评估企业的偿付能力，往往需要从其他银行或金融机构获取企业现有授信额度。为了能够获得企业在多家金融机构的授信总和，可以采用秘密分享技术，在多家机构间实现企业贷款数据的共享。以查询企业 A 在 M 家金融机构的贷款总额为例，每家金融机构先将 A 在本机构的贷款额度分成 N 份（$N \geq M$），再向其他（M–1）机构随机发送其中 1 份。每个机构将剩余 N–M 份数据和从其他机构得到的 M–1 份数据进行求和，再通过开放银行服务将求和结果返回到查询银行，最终查询银行对得到的所有结果再次求和，即可得到 A 企业在 M 家金融机构的贷款总额。依托基于秘密分享技术的开放银行服务，A 企业在各家机构的贷款额度不会被其他机构所获得，充分满足了数据共享的最小可用原则。

（四）基于不经意传输协议的匿踪查询服务场景

用户在使用开放银行接口进行信息查询时，往往不希望透露自己的查询条件以保护隐私，例如，用户在查询股票信息时，不希望透露自己对该股票感兴趣的信息，防止个人偏好被机构获取。在这样的情况下，可以对开放银行的查询接口及相关流程基于不经意传输协议进行改造，使用户可以查到自己想要的信息，但银行方无法获取用户具体的查询条件且无法推测用户的查询目的，以保护用户隐私。这个方案可以有效保障查询者的隐私安全，满足目的限定原则和最小可用原则。

（五）基于混淆电路技术的人脸识别认证场景

如今，实名认证的需求催生了越来越多的人脸识别场景，但是人脸识别的隐私保护问题却一直困扰着用户。在通过开放银行服务对用户的身份进行核验的场景中，可以使用混淆电路技术，使终端所采集的生物识别信息不需要传输到银行端即可得到身份比对结果。例如，在重要证件寄送服务中，快递方在收取费用的同时也需要对用户进行身份核验。通过基于混淆电路技术的开放银行服务，快递方可以先使用终端临时性采集用户人脸特征，并与用户在银行端的人脸特征进行比对，得到核验结果。这种方式避免了终端采集的人脸信息的直接传输，满足了数据安全保障原则和最小可用原则。

五、面临的挑战

尽管隐私计算技术的数据保护功能与开放银行的数据合规要求高度契合，但基于隐私计算的

开放银行场景在实际应用中仍面临着一些数据合规挑战。

（一）数据合规离不开用户的知情同意

隐私计算中的“数据可用不可见”“不共享数据”理念能够避免原始数据的直接交互和共享，但这些理念尚不能完全满足开放银行场景下个人信息保护的全部要求。例如，《民法典》《网络安全法》《个人金融信息保护技术规范》等均规定了收集、处理数据的知情同意原则。如果数据主体对于开放银行参与方处理数据的方式或者处理目的不知情、不同意、未授权，即便隐私计算能够实现数据的可用不可见，也仍存在数据合规的风险。

（二）隐私计算的结果数据权属暂无法律明确规定

权益归属需要以产权明晰为基础。然而，数据作为生产要素，其社会性、关联性的特质使得其实现产权归属的明晰化难度较大。这个过程在基于隐私计算技术的开放银行场景下更加难以实现。例如，在开放银行各参与方共同提供原始数据来训练模型的情况下，通过隐私计算获得的算法模型应当如何在各参与方之间划分权属，进而在各参与方之间进行利益分配，这或许是当前法律亟待解决的问题。

（三）隐私计算离不开可信数据和可信节点

隐私计算在应用到开放银行场景时，其计算结果的真实性、准确性、可靠性依赖于可信数据和可信节点。由于隐私计算是基于数据的计算，数据的质量对计算结果尤为重要，如果在数据共享过程中，参与节点使用了投毒数据进行建模，则隐私计算的结果将变得不可信甚至不安全。另一方面，如果恶意节点作为开放银行中隐私计算的参与方，那么开放银行生态也会受到威胁。因此，数据污染或数据投毒等问题需要得到高度重视并尽可能避免。同时，如何探查和防范恶意节点，以及减小恶意节点的危害，也是一个亟待解决的难题。

六、总结

隐私计算技术在开放银行的信贷风控、产品营销等应用场景中具有广阔发展空间，应进一步加大该技术的研究力度，使其更好地在金融场景中应用。同时，考虑到隐私计算技术只能解决技术层面问题，不能解决开放银行数据应用的合规管理、产权归属问题，例如获得用户的知情同意和授权，确定结果数据的产权归属，以及如何保证其参与节点的可信安全等。因此，开放银行数据合规共享的规模化实现还需要同步推进相应制度和流程建设。

参考文献：

[1] 中国银联技术管理委员会 . 开放银行数据保护与共享研究报告 [R/OL].2021，（10）：21.

[2] Fenghua Li, Hui Li, Ben Niu, Jinjun Chen. Privacy Computing: Concept, Computing Framework, and Future Development Trends[J]. Engineering, 2019，5（6）：1179–1192.

[3] 李凤华，李晖，贾焰，俞能海，翁健 . 隐私计算研究范畴及发展趋势 [J]. 通信学报，2016，37（4）：1–11.

[4] Big Data UN Global Working Group.Un Handbook on Privacy–Preserving Computation Techniques[R/OL].2019.

[5] 龚光庆 . 隐私计算技术在银行业的应用探索 [J]. 中国金融电脑，2021，（10）：36–39.