隐私计算联盟
Privacy Preserving Computing Alliance

隐私计算技术应用合规指南

（2022 年）

隐私计算联盟

2022 年 12 月

引　言

近年来，随着数字经济的发展和数字化转型的深入，企业逐渐积累大量数据，需要与外部数据进行融合以充分释放价值。但是，全球数据安全事件频发，数据保护合规监管日趋严格，企业在数据流通和协作方面的风险及合规成本大大增加。在此双重背景下，企业亟须探索出一条数据安全流通的新道路，在保证数据安全的前提下挖掘数据价值。隐私计算技术因其“数据可用不可见”的特点，为上述困境提供了解决思路。

隐私计算是一类在提供隐私保护的前提下，实现数据价值挖掘的技术，是人工智能、密码学、数据科学等众多领域交叉融合形成的跨学科技术[1]。应用隐私计算，原始数据不出域，参与方也难以逆推原始输入数据，降低了原始数据泄露的风险，进而帮助企业履行安全保障义务，降低数据滥用风险。

近几年，隐私计算发展迅速。据统计，2016 年至 2022 年第一季度，中国隐私计算企业的累计融资额超 30 亿元人民币，资本热度持续提升[2]。根据隐私计算联盟 2022 年发布的《隐私计算产业图谱 1.0》，互联网、大数据、金融科技、AI、区块链、云服务和信息安全等行业的企业都入局隐私计算技术服务产业，金融、政务、通信、互联网、工业及能源、医疗等行业领域均有应用需求。此外，国务院、各中央部委出台的一系列政策文件，如发展改革委等四部委发布的《全国一体化大数据协同创新体系算力枢纽实施方案》等，以及《上海市数据条例》等地方性法规等也开始将隐私计算作为一种数据流通过程中的

[1] 闫树，吕艾临：《隐私计算发展综述》，载《信息通信技术与政策》，2021 年第 6 期，第 1 页。
[2] 艾瑞咨询 2022 年《中国隐私计算行业研究报告》第 13 页。

安全保障技术来鼓励使用。

然而，在火热的发展势头下，隐私计算的应用也面临着一些挑战，在合规方面尤为明显。一方面，近年来我国的数据合规监管趋严，立法愈发频繁，企业的数据合规意识也逐渐建立，对数据合规问题的关注度提升。另一方面，随着《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）的出台和生效，个人信息的处理行为面临着更严格的法定义务和法律责任约束，隐私计算应用于处理个人信息时也必须考虑如何遵守相应要求。而在现阶段，企业对于授权同意、个人信息保护影响评估以及个人信息权利保障等合规义务如何落地仍然存在一些疑惑，如何在匹配《个人信息保护法》合规要求的同时尽可能降低合规对业务的影响，仍有待探索。因此，在相关实施细则出台和监管执法案例出现之前，很多需求方对隐私计算技术应用持谨慎的观望态度，行业内对于隐私计算应用的合规性展开了一些讨论，对于法律规定的合规要求也产生了一些理解和认识上的偏差。

对此，隐私计算联盟、中国信通院云计算大数据研究所和多家企业共同完成了《隐私计算技术应用合规指南（2022 年）》。在期待立法不断完善、实践不断创新的同时，我们尝试在我国现有立法框架下，对隐私计算技术应用的合规问题进行探索和梳理，对隐私计算技术面临的合规挑战进行分析，并提出一些合规要点，希望对现阶段的隐私计算技术应用提供一些合规指引和参考、为未来行业的规范和立法的完善提供一些思路。

目　录

表 目 录

图 目 录

第一章

概述

(一) 隐私计算技术的概念和原理

隐私计算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”[3]。**主流的隐私计算技术可以分为三大方向：**一是以**多方安全计算**为代表的基于密码学的隐私计算技术，二是以**联邦学习**为代表的人工智能与隐私保护技术融合衍生的技术，三是以**可信执行环境**为代表的基于可信硬件的隐私计算技术[4]。

多方安全计算可以在各方不泄露输入数据的前提下完成多方协同分析、处理和结果发布，因此广泛应用于联合统计、联合查询、联合建模、联合预测等场景。**联邦学习**能够在本地原始数据不出库的情况下，通过对中间加密数据的流通与处理来完成多方联合的机器学习训练，因此广泛应用于联合建模，也可与可信执行环境配合使用，提供安全性、应用性更强的综合解决方案。**可信执行环境**通过软硬件方法在中央处理器中构建一个安全的区域，保证其内部加

[3] 隐私计算联盟、中国信通院云大所《隐私计算法律与合规研究白皮书（2021 年）》。
[4] 隐私计算联盟、中国信通院云大所《隐私计算白皮书（2021 年）》。

载的程序和数据在机密性和完整性上得到保护，可以完成对多方数据完成联合统计、联合查询、联合建模及预测等各种安全计算[5]。

(二) 隐私计算技术合规讨论的产生原因

在我国，隐私计算技术应用的合规在行业内引发了热烈的讨论，原因主要有以下几点：

多主体参与导致法律关系复杂。从法律主体看，隐私计算技术应用往往会涉及多个参与方共同协作，数据提供方、技术提供方、结果使用方是最为常见的三类主体。**数据提供方**一般是指在隐私计算技术应用过程中提供数据的主体。**技术提供方**一般是指提供数据处理平台、算法工具、解决方案等技术支持的主体。**结果使用方**一般是指获取隐私计算最终输出的数据结果并进行场景应用的主体。在实践中，还存在数据提供方本身不只一方、各参与方角色重合等情况。因此，一个隐私计算应用场景中往往包含多对法律关系，各参与方角色的重合还会带来数据合规义务的竞合或抵消。倘若不能准确判断各方之间的法律关系或明确法律义务或法律责任，就会引发一些合规问题。

受疫情影响，某快递公司“先寄后付”业务深受客户追捧，但仅依靠快递公司内部用户数据无法准确判断客户是否为低风险用户，若判断失误，容易引发坏账风险。故在第三方隐私计算技术提供方的协助下，该快递公司引入某大型银行信用卡中心掌握的用户在金融业务中的个人信用相关行为和跨行数据，通过联合建模建立散单客户风险识别模型。

在上述案例中，银行信用卡中心为数据提供方，快递公司同时为数据提供

[5] 隐私计算联盟、中国信通院云大所《隐私计算白皮书（2021 年）》。

方和结果使用方，技术提供方为第三方隐私计算技术服务方。

隐私计算技术在我国的合规价值缺乏背书。隐私计算技术包含多种数据处理行为，各参与方应当遵守我国数据合规相关法律法规。尽管目前我国数据合规法律的基本框架已初步建立，但配套的实施细则尚不完备，可供参考的司法和执法案例较少。相比之下，国外在立法和监管方面提供了更明确细致的指引。欧洲数据保护委员会（EDPB）发布的《关于第 25 条的设计和默认数据保护指南》在建议部分指出，有条件的使用隐私增强技术可以作为满足欧盟《通用数据保护条例》（GDPR）第 25 条规定的保护措施[6]。这在某种程度上从监管的角度赋予了隐私计算技术能够帮助履行合规义务的法律地位[7]。但目前在我国，隐私计算技术的合规价值尚未得到类似的背书。**实际上，隐私计算技术的合规价值会因法律体系、社会和经济背景的不同而有所不同。在立法方面，**尽管我国的《个人信息保护法》在立法原则上与欧盟《通用数据保护条例》有共通之处，但具体的法律规定存在很多差异。因此，隐私计算技术在欧盟得到认可的合规价值，放置在我国的法律体系下并不天然成立。**在社会和经济背景方面，**隐私计算在欧洲的推广主要得益于隐私保护问题亟待解决，其本身就带有一定的合规属性；而隐私计算在我国的快速发展主要是因为能够促进数据流通，

[6] 见 Guidelines on Article 25 Protection by Design and by Default 第 30 页。EDPB 指出，最先进的隐私增强技术（Privacy-enhancing technologies）可以被视为 GDPR 第 25 条要求采取的措施（如果适用于基于风险的方法）。使用隐私增强技术本身不一定能完全履行 GDPR 第 25 条规定的义务，数据控制者应当评估该措施在实施数据保护原则和数据主体权利方面是否适当有效。

[7] 欧洲数据保护委员会 （EDPB）是根据《通用数据保护条例》（GDPR）的规定设立的独立机构，其任务和职责包括提供一般指导（包括指南、建议和最佳实践）以澄清法律并促进共识或推动欧盟的数据保护法律的实施等。

其价值更多的体现在促进社会经济发展层面。基于以上差异，隐私计算技术在我国的合规价值，需要基于我国的具体情况进行研究和讨论。

技术与法律对于相同问题的认知存在差异。隐私计算技术的合规分析，涉及技术与法律两大专业领域的碰撞与融合。对法律专家而言，判断隐私计算技术的合规性，需要理解通过技术语言描述的数据处理行为，将其与法律条文的规定相对应，进而判断相关行为属于何种法律行为，会触发何种合规风险。对技术专家而言，了解隐私计算技术应用合规性，也需要经历从技术到法律的认知转变。这种涉及跨专业的沟通往往会引发一些认识和理解上的偏差，进而导致关于合规问题的一些争议和讨论。

(三) 隐私计算技术的法律适用

讨论隐私计算技术应用的合规问题，首先需要明确法律适用，厘清法律关系。尽管我国数据保护领域的相关立法尚不完备，但现有法律框架基本可以涵盖隐私计算应用所涉及的法律行为。各参与方需根据隐私计算应用的场景进行具体的判断和分析。

隐私计算技术应用本质上是一种数据处理行为，各方在隐私计算技术应用涉及的数据提供、加工、传输、使用等环节的数据处理行为，均适用相关法律法规对于数据处理的要求。

首先，应用隐私计算技术应当遵守《中华人民共和国民法典》[8]

[8] 《中华人民共和国民法典》第四编“人格权”第六章“隐私权和个人信息保护”。

《中华人民共和国刑法》[9]等**综合性立法以及相关司法解释**[10]中对于个人信息保护和数据保护的相关要求，违反相关规定将视情节承担相应的民事或刑事责任。

其次，应用隐私计算技术应当遵守数据合规领域的专门规定。2021 年，《中华人民共和国数据安全法》（以下简称“《数据安全法》”）和《个人信息保护法》相继正式出台并生效，与此前的《中华人民共和国网络安全法》（“《网络安全法》”）共同构成了**我国数据合规领域的基本法律架构。**2022 年 9 月 12 日，国家互联网信息办公室发布了《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》，拟修订后的《网络安全法》与《个人信息保护法》《数据安全法》的衔接更加严密合理。违反《网络安全法》《数据安全法》和《个人信息保护法》的相关规定将根据不同情节承担暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照、高额罚款等行政责任。

同时，应用隐私计算技术应遵循相关国家标准、行业标准中对于数据处理行为的细节要求，如《信息安全技术 个人信息安全规范（GB/T 35273-2020）》《信息安全技术 个人信息去标识化指南（GB/T 37964-2019）》等。

此外，若隐私计算技术应用涉及特殊监管行业，如金融、医疗、

[9] 《中华人民共和国刑法》第二百五十三条之一、第二百八十五条、第二百八十六条、第二百八十七条之二等。

[10] 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》《关于加强刑事检察与公益诉讼检察衔接协作严厉打击电信网络犯罪加强个人信息司法保护的通知》等。