

汉坤法律评述

2026 年 8 月 17 日

北京 | 上海 | 深圳 | 杭州 | 武汉 | 海口 | 香港 | 新加坡 | 纽约 | 硅谷 | 伦敦

云上方圆（一）：从 IaaS 到 MaaS — 云服务的法律关系与监管图谱

作者：权威 | 陈程 | 郑博 | 黄思颖

一、写在开篇

经过多年发展，云服务已经成为企业数字化经营的重要基础。企业的数据处理、应用运行、系统管理以及人工智能能力调用，都可能通过云端完成。2015 年，国务院在《国务院关于促进云计算创新发展培育信息产业新业态的意见》（国发[2015]5 号）中，将云计算界定为推动信息技术能力按需供给、促进信息技术和数据资源充分利用的“全新业态”。此后，云计算逐步由基础资源的集中部署，向平台化、服务化、行业化和智能化发展。

市场数据也反映了这一变化。根据中国信通院发布的《云计算蓝皮书（2025 年）》，2024 年我国云计算市场规模达到 8288 亿元，同比增长 34.4%。工业和信息化部发布的 2025 年软件业运行情况显示，2025 年云计算、大数据服务实现收入 16230 亿元，同比增长 13.6%。尽管两项数据的统计口径并不相同，但均表明云服务已经形成相当规模的市场。

市场规模扩大的同时，云服务的具体形态也在不断丰富。除传统的 IaaS、PaaS 和 SaaS 外，人工智能的发展进一步催生了 AI IaaS、AI PaaS、MaaS、AI SaaS、AIMSP 等服务形态。《云计算综合标准化体系建设指南（2025 版）》（工信部联科[2025]175 号）也将云服务的范围扩展至基础设施即服务、平台即服务、数据即服务、软件即服务、人工智能即服务、安全即服务，以及面向云计算系统建设和应用全过程的生命周期管理服务。

不同的云服务形态实际提供的能力和采用的交易结构可能存在较大差异，所涉及的市场准入、监管规则、知识产权、数据安全、服务保障和责任分配问题也呈现出显著区别。

因此，对云服务法律问题的讨论，需要从具体的服务内容和交易结构出发，进一步判断各方形成了何种合同关系、分别控制哪些资源和能力，以及应当承担哪些义务。本篇将先对云服务的主要类型、常见合同形态和核心法律关注事项作一梳理，为后续结合具体监管制度和业务场景展开讨论建立基础。

二、云服务的主要类型及合同关注要点

从技术和商业实践来看，云服务通常分为 IaaS、PaaS 和 SaaS；在人工智能场景下，又进一步延伸出 MaaS 及其他 AI 云服务。不同服务形态对应不同的服务内容、控制范围和责任边界。

（一）IaaS：持续提供基础资源能力

1. 业务实质

IaaS 的核心，是将计算、存储、网络等基础信息技术资源持续提供给客户使用。

- **服务形式：**IaaS 服务提供方通常向客户提供云服务器、对象存储、云硬盘或算力租赁等服务；
- **法律关系：**服务提供方负责底层资源的组织、运行和维护，客户通常仍控制操作系统、应用部署、权限体系、数据处理逻辑和上层业务功能。

2. 合同关注要点

IaaS 并非简单的“设备租赁”。服务提供方持续承担资源可用义务，客户则控制系统配置、应用运行和业务数据。故障责任、数据安全责任、可用性承诺义务和服务中断损失如何分配，需要结合双方实际控制范围和合同约定判断。

（二）PaaS：持续提供运行环境和平台能力

1. 业务实质

- **服务形式：**PaaS 不仅提供底层资源，还会提供开发、部署、运行、调度、数据库、中间件、容器和接口管理等平台能力。
- **法律关系：**与 IaaS 相比，PaaS 服务提供方对运行环境和关键技术要素的控制更深。客户虽然仍控制业务逻辑，但在接口规则、版本演进、底层技术选择和系统迁移方面会更依赖平台。

2. 合同关注要点

与传统系统开发更关注系统能否最终交付并通过验收不同，PaaS 是一项长期服务，客户实质上将部分技术决策权交给了服务平台方，所以其合同更关注平台规则能否变更，以及变更是否会影响业务连续性。关于平台规则、兼容责任、技术锁定、协同义务和迁移安排的约定，会直接影响合同双方在服务调整、故障处置或平台退出时的责任。

（三）SaaS：持续提供软件功能

1. 业务实质

SaaS 是商业实践中最常见的云服务形态，但往往被非专业人士简单理解为“在线软件”或“账号开通”的一类服务。

从服务实质来看，SaaS 核心仍然是提供软件功能而非提供软件产品。服务提供方在其控制的基础设施和运行环境中，持续向客户提供软件功能，客户取得的是持续使用功能的权利，并不因此取得软件产品的所有权。

2. 合同关注要点

与传统软件销售相比，SaaS 合同更需要关注以下问题：

- 持续可用性如何界定；
- 功能变更是否受限；

- 客户数据与日志的访问范围如何确定；
- 服务终止后数据导出和迁移是否具备现实可操作性；以及
- 服务提供方能否依据在线规则单方调整服务内容。

（四）MaaS 及其他 AI 云服务：持续提供人工智能能力

人工智能的发展已经突破了传统 IaaS、PaaS 和 SaaS 的三分框架。中国信通院在《云计算蓝皮书（2025 年）》中，将当前人工智能时代的云服务模式发展趋势概括为 AIaaS、AIPaaS、MaaS、AISaaS、AIMSP 等；《云计算标准化体系指南》也将人工智能即服务单列为一类云服务。云服务提供的对象，正在从通用资源和软件功能延伸至分层的人工智能能力。与传统云服务相比，MaaS 及其他 AI 云服务的履约链条更长，责任归属也更复杂、细致。客户表面上购买的可能只是模型调用、推理、智能体编排或某项 AI 应用，但背后往往叠加了底层算力、模型、日志处理、内容安全和监控组件等多层服务。

因此，合同相对方未必是唯一的实际履约方。判断监管责任、数据义务和合同风险时，需要沿服务链条逐层分析。

（五）其他常见云服务类型

除上述典型类型外，市场上还普遍存在 MSP（Managed Service Provider，托管服务提供商）、实施服务和系统集成服务等安排。这些主体以不同方式参与云服务的部署和运营。

此类服务提供方未必直接提供底层云资源，但往往会深度参与系统部署、基础运维、资源优化和安全管理，在很大程度上影响云服务能否在客户侧实际落地。这类服务的参与主体较多、履约链条较长，明确各环节参与主体及其角色，有利于在争议发生时合理划分各方责任。

三、云服务的主要监管要求

IaaS、PaaS 和 SaaS 是商业和技术分类，并非现行法规直接采用的监管分类。监管机关在实施监管或执法时，通常从具体业务行为入手确定服务性质，例如是否提供数据存储、应用运行环境、互联网信息服务或网络接入。因此，判断云服务的监管要求，仍需先识别具体服务内容和参与主体，再分别适用对应规则。

（一）云服务提供方：重点关注准入与持续运营要求

1. 准入监管

云服务提供方可能涉及行业准入要求，但并非所有云服务均当然需要取得特定许可。具体仍应根据实际服务内容判断。

常见的准入要求包括：

（1）增值电信业务许可 — B11 互联网数据中心（IDC）业务

提供 IaaS、PaaS 能力的云服务商，通常首先需要关注 B11 互联网数据中心业务许可。

IaaS、PaaS 的常见产品包括弹性计算、云存储、对象存储、云硬盘、负载均衡、中间件、消息队列和应用开发平台。这类服务通常利用数据中心的设备和资源，通过互联网或其他网络，为用户提供数据存储、应用开发环境、应用部署和运行管理等能力。

按照《电信业务分类目录》，上述服务通常会落入 B11 互联网数据中心业务项下的互联网资源协作服务。服务提供方应在该类业务展业前取得相应的增值电信业务经营许可。

(2) 增值电信业务许可 — B25 信息服务（ICP）业务

云服务商提供 SaaS 服务时，还需要结合具体功能判断是否涉及 B25 信息服务业务。

SaaS 侧重于持续提供软件功能。其是否需要取得 B25 信息服务业务许可，不能仅以在线收费或订阅制作为判断标准，而应审查服务实质是否属于通过互联网向用户提供信息发布、信息搜索、信息交互、信息处理、信息保护等信息服务。涉及新闻、出版、教育等特定内容的，还需进一步关注内容主管部门的前置审批或专项许可要求。

如果相关 SaaS 并不构成互联网信息服务，可能不落入 B25 监管范围；如果还提供在线交易或数据处理平台等功能，则可能涉及 B21 在线数据处理与交易处理（EDI）业务。最终仍需结合产品功能和交易结构个案判断。

此外，云服务商提供下载加速、企业专网、专线接入或机房带宽接入等服务的，还可能分别涉及 B12 内容分发网络（CDN）、B13 国内互联网虚拟专用网（IP-VPN）或 B14 互联网接入服务（ISP）等许可。

2. 运营监管

云服务商既可能作为网络运营者开展网络运行、数据处理和个人信息处理活动，也可能作为 IDC 业务经营者接触或承载客户数据。因此，除取得相应许可外，还需持续履行网络安全、数据安全和客户数据保护义务。

根据《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全条例》《工业和信息化领域数据安全管理办法（试行）》以及《工业和信息化部办公厅关于加强互联网数据中心客户数据安全保护的通知》（工信厅网安[2025]5 号）等规定，云服务商在运营过程中需要持续关注的主要要求如下。

从 IaaS 到 MaaS——云服务的法律关系与监管图谱

HANKUN

义务类型	义务事项
网络安全义务	按照网络安全等级保护制度的要求，履行网络安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改
基础数据合规义务	在网络安全等级保护制度的基础上，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
个人信息保护义务	对个人信息处理活动负责，采取必要措施保障所处理个人信息安全；处理活动应遵循合法、正当、必要与诚信原则，并坚持“合法正当、最小必要、目的明确”的要求
特有客户数据安全保护义务	- 对于党政机关等重点客户，依据客户类别和数据保护需求，提供差异化安全防护能力，并配合采取相应保护措施，提升 IDC 承载信息系统和数据的安全保护能力 - 配合客户建立访问控制策略，配备技术措施防范客户数据未经授权访问等安全风险 - 健全客户数据操作登记、权限审批、账号动态核验等机制；明确客户数据销毁安全策略和操作规程，未经授权不得擅自销毁客户数据 - 提供物理、逻辑等数据隔离方式 - 建立覆盖网络与设备更换、运维、升级，以及数据迁移等可能导致客户重大数据安全风险的高危操作台账，并于事前取得客户授权
对外责任约定	- 在与客户签署的合同协议中，参照有关行业标准，根据业务模式和服务内容，明确双方数据安全保护责任义务 - 涉及通过采购第三方服务商设备、服务等，处理客户数据的，需明确各方数据安全保护责任义务 - 加强对重点客户的数据安全风险提示
业务可用性与安全保障	- 通过冗余设计等，提高业务连续性和稳定性 - 因 IDC 业务经营者原因引发客户数据安全事件的，立即启动应急处置，及时告知客户，并结合事件影响程度，根据相关法规和标准要求向电信主管部门报告，根据事件类型、级别等，及时配合客户开展事件应急处置和上报 - 提供多样化的安全保障措施，包括数据加密、脱敏、访问控制、鉴权与校验、日志记录与审计、数据备份与恢复等数据安全技术能力，以及防火墙、堡垒机、非法入侵检测、防篡改、漏洞扫描、病毒防范、安全升级等网络安全防护产品或服务供客户选择
特殊场景保障能力	- 资源监控和负载均衡：配备存储和计算资源监控技术能力、存储和计算资源负载均衡技术能力，及时发现资源异常使用情形，保障资源安全可用 - 涉及提供人工智能训练数据集管理功能的，需提供保障客户自有训练数据集安全的能力，避免客户自有训练数据集被泄露、污染

- 云服务商应持续关注的监管要求 -

云服务商为党政机关等特殊客户提供服务的，还需结合《云计算服务安全评估办法》等规定，判断是否应当完成安全评估，并履行相应的安全、应急响应和风险处置义务。

（二）云服务使用方：重点关注行业限制与自身合规义务

一般而言，单纯使用云服务不会产生独立的前置许可义务。但是，特定行业可能对是否可以上云、可以使用何种云以及如何管理云服务外包设有专门要求。对于使用方而言，使用云服务并不会减轻其原有的数据合规和行业监管义务。

1. 行业限制

以下以金融机构和党政机关、关键信息基础设施运营者（CIIO）为例：

- 金融机构使用云服务时，通常需要结合系统重要性、数据敏感程度和金融监管要求确定部署方式。涉及金融云的，还需关注金融云服务标准符合性自律管理及相应金融监管规则。

因此，金融机构是否上云，除了云服务采购问题之外，还可能构成信息科技外包管理的一部分。对于核心系统和敏感数据，部署方式、服务商选择和持续监督通常需要接受更严格的审查。

- 党政机关和 CIIO 采购使用面向其提供服务的云平台时，需要关注相关云平台是否通过云计算服务安全评估。评估重点包括云服务商的征信和经营状况、关键岗位人员稳定性、供应链安全、平台防护、客户数据迁移、业务连续性等因素。

其他特殊行业也可能对云服务商选择和云服务使用设有专门要求，需要结合具体行业规则判断。

2. 通适义务

使用云服务不意味着使用方可以将自身责任一并外包。使用方通常需要通过供应商管理、合同约定和持续监督，确保云服务满足其自身适用的合规要求。例如，使用方开展数据处理活动，仍需建立全流程安全管理制度并依法处理个人信息；使用方属于 CIIO 的，发生重大网络安全事件、发现重大网络安全威胁或出现运营中断等情形时，还需按规定向有关主管部门报告。

此外，使用方在采购阶段就应当明确云服务的商业和技术要素，并对服务使用、变更、退出和责任追究作出可执行的合同安排。

四、结语

云服务涵盖基础设施、平台能力、软件应用和人工智能服务等多种形态。不同服务的交付内容和技术架构各有差异，各参与方对基础设施、系统、应用和数据的控制程度也不相同，由此形成不同的合同关系、监管要求和责任边界。

因此，在具体项目中，对云服务的法律分析仍需落实到交易结构本身，以进一步判断所需资质、适用规则和合同安排，并形成与实际业务相匹配的责任分配机制。

后续我们将继续对云服务的业务准入、持续运营、合同安排、服务退出和责任承担等问题进行探讨与分析。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

权威

电话： +86 21 6080 0946

Email: wei.quan@hankunlaw.com

陈程

电话： +86 21 6080 0992

Email: cheng.chen@hankunlaw.com