

# 安全风险视域下的云平台责任界定与治理探析



## 一 云平台安全风险域与安全责任

### （一）云平台及其安全风险域

云计算作为随着信息技术演进而出现的一种新型生产和服务模式，能够按需配置和优化一种或多种昂贵的计算资源，实现资源的有效整合，促进生产效率提升，创新数字经济商业模式。市场调研公司 Gartner 的数据显示，2018 年全球公共云服务市场规模为 1824 亿美元，到 2022 年全球公有云服务营收将增长至 3312 亿美元。<sup>[1]</sup>

在全球云服务市场，存在产业相互依存与用户层级嵌套的现象，“服务商—用户”身份可随着产业链延伸而不断衍化（见图 1）。本文所指的云平台服务商是指管理、运营、支撑云计算的基础设施及软件，并通过网络交付云计算资源的供应方；云平台用户是指直接使用云计算服务，并同云平台服务商建立业务关系的参与方；而云计算平台即云平台，则是云平台服务商提供的云计算基础设施及其上的服务软件的集合。<sup>[2]</sup>

图 1 本文研究的“云平台服务商—云平台用户”范围

以云平台服务商提供的资源类型划分，云平台主要有三种服务模式（见图 2）：基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。在 IaaS 模式下，云平台是作为网络基础设施存在的，云平台服务商向用户提供虚拟计算机、存储、网络等计算资源及访问云平台的服务接口，用户可在这些资源上部署或运行操作系统、中间件、数据库和应用软件等；在 PaaS 模式下，云平台主要作为软件开发和运行平台，云平台服务商向用户提供标准语言与工具、数据访问、通用接口等，用户可利用该平台开发和部署软件；在 SaaS 模式下，云平台主要作为应用软件，云平台服务商向用户提供的是运行在云计算基础设施上的应用软件，用户无须自行开发软件，可利用不同设备上的用户端（如 Web 浏览器）或程序接口直接使用云平台服务商提供的应用软件。

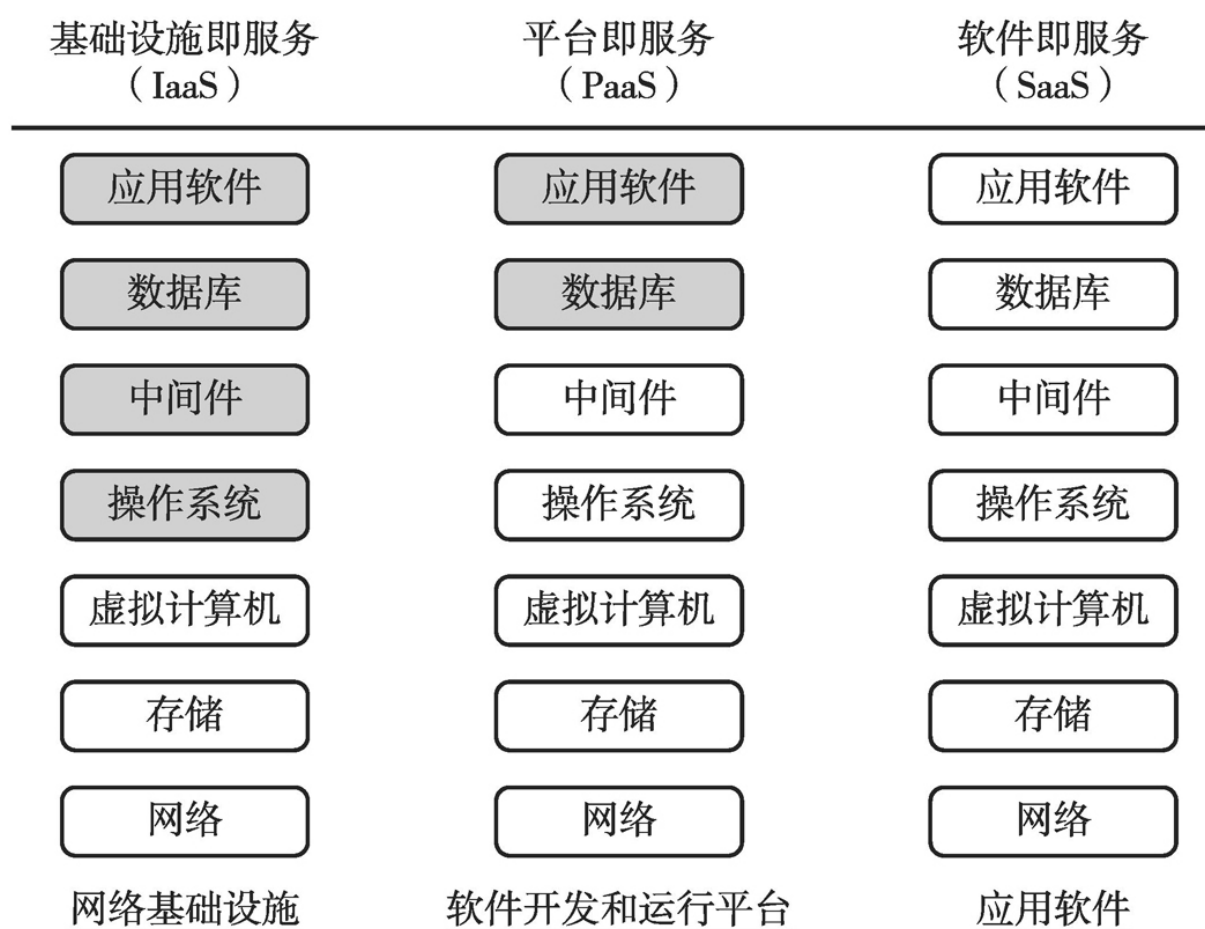


图 2 云平台三种服务模式

在不同的云平台服务模式和运营方式中，潜藏着各种安全风险，深刻影响了云平台的广泛应用，可谓“牵一发而动全身”。具体来看，这些安全问题涉及如下四个安全风险域。

## 1. 系统安全

系统安全涵盖保障和支撑云平台运行的通信、软件、硬件等一系列基础设施的安全域，如云主机安全、虚拟化平台安全、通信安全及运行环境安全。其中，资源虚拟化技术是云平台的特有基础技术之一，需关注虚拟化软件的脆弱点、主机虚拟化后容器安全及其日常管理安全等风险。由于虚拟化环境独特的动态特性，在遇到虚拟机未能激活、资源冲突、虚拟系统通信中断等问题时，传统的静态安全防护措施往往无法奏效。

## 2. 应用安全

应用安全涵盖预防与管控在云平台中部署的与业务相关的应用或应用开发接口所带来风险的安全域，包括业务应用系统在设计、开发、发布及配置等过程中所应采取的安全措施，也包括应用在上线运行后所采取的业务防护措施，如应用识别、入侵防御、身份认证及资源访问控制等，还包括业务应用的基础支撑软件和应用扩展（APIs）的防护、加固，以及访问业务应用或调用应用扩展的操作终端的安全管理与控制等。

### 3. 数据安全

数据安全虽然不是云环境下所特有的安全问题域，但是云平台用户最关心的关键安全问题之一。数据作为云平台的核心资源，按来源可分为三类：一是用户在云平台业务系统中生产的数据，二是由用户操作业务系统的行为而产生的数据，三是来自通信、平台及应用等因运行而产生的系统运维数据。云平台的数据安全应确保数据在传输、存储、流动、应用等环节中风险可控。当前云平台用户的数据安全对云平台服务商的管控能力高度依赖，用户业务数据的权属和管理虽属于用户本身，但其对数据保护和数据管理的能力有待提升。

### 4. 内容安全

内容安全是在云平台中所承载的业务运营结果或其数据所附着的信息的防护或监管的安全域，这些内容最终往往以图片、文本、视频、声音等形式呈现。依据安全管控的目标不同，可分为合法内容的保护和非法内容的监管与打击。前者主要包括商业秘密保护、版权保护、复制防护等，后者通常涉及云平台上可能潜藏的色情、暴力、低俗、政治敏感、恶意广告等违法违规或有害内容，这些也是当前云平台中最常见、最难监管、防控难度较大的安全问题之一，轻则影响业务平稳运营，重则造成巨大社会舆论压力，导致云服务被暂停甚至中止。

#### （二）云平台安全责任概念界定

为解决日益凸显的云平台安全问题，云平台安全责任的落实与划分至关重要。如图 3 所示，与云平台相关的责任主体包括监管部门、云平台服务商和云平台用户，其相关的安全责任一方面是来自监管部门对云平台服务商的责任要求，另一方面则是云平台服务商与云平台用户之间的责任划分问题。

图 3 本文研究的“云平台安全责任”范围

其中，监管部门对云平台服务商的安全责任要求为：一是行业准入与资质管理，即国家对电信业务经营实行许可制度，云平台服务商需要依据相关规定取得《增值电信业务经营许可证》，开展云平台涉及互联网资源协作服务、互联网内容分发服务、互联网接入服务、互联网域名解析服务等电信业务；二是云平台服务商需依据法律法规合规开展业务。而云平台服务商与云平台用户的责任关系主要涉及：一是依据合同关系划分责任，二是在侵权关系下依据不同情境进行责任界定。

本文研究的重点是根据在系统安全、应用安全、数据安全、内容安全四个安全风险域下，监管部门对云平台的监管要求，界定云平台服务商基于合规的安全责任，以及云平台服务商与云平台用户的责任划分。可以发现，云平台安全涉及责任主体的多样性、平台服务模式的多样性以及部署方式的特殊性，再加上不同场景的合规需求差异巨大，以及国内外不同的监管要求，导致云平台服务商和云平台用户之间的安全责任难以清晰界定，这也进一步说明了云平台安全治理的复杂性与艰巨性。

二 云平台安全责任的国内外监管

（一）国内核心法规与监管要求梳理

根据《电信业务分类目录（2015 版）》的相关分类，云平台涉及互联网资源协作服务、互联网内容分发服务、互联网接入服务、互联网域名解析服务等电信业务，并建立了较为完善的法律法规监管体系（见图 4）。

图 4 云平台安全责任法律法规与监管体系

其中，《网络安全法》、《计算机信息网络国际联网安全保护管理办法》（公安部第 33 号令）、《电信条例》、《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）等对云平台在系统安全、应用安全、数据安全、内容安全等方面提出了相关的要求（见表 1），具体有：①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对用户违法行为配合处置；⑤违法内容监测处置；⑥安全风险向有关部门报告；⑦执法技术协助；等等。此外，《侵权责任法》《信息网络传播权保护条例》《互联网信息服务管理办法》等法律也从不同角度对云平台安全责任有所覆盖。但是，当前法律法规对于云平台服务商和云平台用户的安全责任划分仍待进一步研究。

| 表 1 国内云平台安全相关政策文件 |          |        |       |                     |                                  |
|-------------------|----------|--------|-------|---------------------|----------------------------------|
| 序号                | 政策/法规/标准 | 云平台服务商 | 云平台用户 | 涉及的云安全域             | 对云平台具体监管要求                       |
| 1                 | 《网络安全法》  | 网络运营者  | 个人或组织 | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对 |

|  |  |  |  |  |                  |
|--|--|--|--|--|------------------|
|  |  |  |  |  | 用户违法行为<br>配合处置；⑤ |
|--|--|--|--|--|------------------|

|   |                              |               |              |                |                                                                     |
|---|------------------------------|---------------|--------------|----------------|---------------------------------------------------------------------|
|   |                              |               |              |                | 违法内容监测处置；⑥安全风险向有关部门报告；⑦执法技术协助                                       |
| 2 | 《全国人民代表大会常务委员会关于加强网络信息保护的決定》 | 网络服务提供者       | 用户           | 系统安全、数据安全、内容安全 | ①网络安全防护；②网站/App 实名备案审核；③针对用户违法行为配合处置；④违法内容监测处置；⑤安全风险向有关部门报告；⑥执法技术协助 |
| 3 | 《电信条例》                       | 电信业务经营者（增值业务） | 电信用户         | 内容安全、系统安全      | ①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对用户违法行为配合处置；⑤安全风险向有关部门报告             |
| 4 | 《计算机信息系统安全保护条例》              | 计算机信息系统的使用单位  | 计算机信息系统的使用单位 | 系统安全、数据安全      | ①网络安全防护；②安全风险向有关部门报告                                                |
| 5 |                              |               | 服务对象         | 内容安全           |                                                                     |

|   |                                   |                                 |        |                     |                                                                           |
|---|-----------------------------------|---------------------------------|--------|---------------------|---------------------------------------------------------------------------|
|   | 《信息网络传播权保护条例》                     | 网络服务提供者                         |        |                     | 针对用户违法行为配合处置                                                              |
| 6 | 《计算机信息网络国际联网安全保护管理办法》（公安部第 33 号令） | 互联单位、接入单位、使用计算机信息网络国际联网的法人和其他组织 | 单位和个人  | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对用户违法行为配合处置；⑤违法内容监测处置；⑥安全风险向有关部门报告；⑦执法技术协助 |
| 7 | 《公安机关互联网安全监督检查规定》（公安部令第 151 号）    | 网络服务运营机构（互联网接入、域名服务、内容分发服务）     | 联网使用单位 | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对用户违法行为配合处置；⑤违法内容监测处置；⑥安全风险向有关部门报告；⑦执法技术协助 |
| 8 | 《电信业务经营许可管理办法》（工业和                | 增值电信业务经营者                       | 单位或者个人 | 系统安全、内容安全           | ①网络安全防护；②网站/App 实名备案                                                      |

|  |          |  |  |  |      |
|--|----------|--|--|--|------|
|  | 信息化部第 42 |  |  |  | 审核：③ |
|--|----------|--|--|--|------|

|    |                               |            |             |                     |                                                        |
|----|-------------------------------|------------|-------------|---------------------|--------------------------------------------------------|
|    | 号令)                           |            |             |                     | 违法内容监测处置；④安全风险向有关部门报告                                  |
| 9  | 《非经营性互联网信息服务备案管理办法（试行）》       | 互联网接入服务提供者 | 非经营性信息服务提供者 | 系统安全、内容安全           | ①网站/App 实名备案审核；②日志留存；③违法内容监测处置；④安全风险向有关部门报告            |
| 10 | 《互联网信息服务安全管理及使用及运行维护管理办法（试行）》 | 电信业务经营者/企业 | 服务对象        | 系统安全、数据安全           | ①网络安全防护；②日志留存；③安全风险向有关部门报告；④执法技术协助                     |
| 11 | 《关于加强党政部门云计算服务网络安全管理的意见》      | 云计算服务商     | 党政部门        | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②安全风险向有关部门报告                                   |
| 12 | 《云服务协助调查取证安全管理要求》             | 云服务提供者     | 用户          |                     | ①网络安全防护；②网站/App 实名备案审核；③日志留存；④针对用户违法行为配合处置；⑤违法内容监测处置；⑥ |

|    |                                         |      |       |                     |                                            |
|----|-----------------------------------------|------|-------|---------------------|--------------------------------------------|
|    |                                         |      |       |                     | 安全风险向有关部门报告；<br>⑦执法技术协助                    |
| 13 | 《信息安全技术 云计算服务安全指南》<br>(GB/T 31167-2014) | 云服务商 | 云服务客户 | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②梳理了云计算服务安全管理的主要角色及责任              |
| 14 | 《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)  | 云服务商 | 云服务客户 | 系统安全、应用安全、数据安全、内容安全 | ①网络安全防护；②梳理了云计算应用场景中不同服务模式云平台服务商和用户的安全管理责任 |



Excel 下载

表 1 国内云平台安全相关政策文件

(二) 监管要求下的云平台安全责任界定与难点分析

1. 系统安全责任

系统安全责任一方面来自因内部因素导致系统出现问题而形成的安全责任，另一方面也存在资质问题等外部因素带来的安全责任。由此，国内监管政策也基于内外部因素来界定主体安全责任，但其在网络安全防护、实名备案等方面的责任界定上仍存在难点。

我国《网络安全法》第十条、第二十一条、第二十四条，《全国人民代表大会常务委员会关于加强网络信息保护的決定》，《电信条例》第五十九条，《计算机信息网络国际联网安全保护管理办法》（公安部第 33 号令）第十条，《公安机关互联网安全监督检查规定》（公安部令第 151 号）第十条，《非经营性互联网信息服务备案管理办法（试行）》第十条、第十九条，《电信业务经营许可管理办法》（工业和信息化部第 42 号令）第二十六条，《通信网络安全防护管理办法》第五条、第十三条，《计算机信息系统安全保护条例》第十三条等，对云平台的系统安全责任做出了较为明确的规定。其中，云平台服务商须取得经营资质，依据网络安全等级保护制度的要求，承担云平台本身的网络安全防护，保障云平台的系统安全，并对用户使用其服务前进行实名审核，记录备案信息、及时报告系统风险等安全责任，而用户须履行实名备案责任。

然而，监管部门在不同情境中对主体安全责任进行界定，仍面临一定的挑战。如在网络安全防护方面，近年来利用云服务器来进行 DDoS 攻击的事件频发，许多云平台服务商提供基础的防御外部 DDoS 攻击的安全防护能力或服务，以保护处于云计算平台网络中的各类资源不受来自此类攻击的影响，这其中涉及用户授权、操作或者购买。用户有责任维护并管理已购买的自身的业务系统安全，类似如因用户管理不当造成的云主机主动或被动向外发起恶意攻击（如 DDoS 攻击、网络嗅探、病毒木马攻击等）的情况，其主要安全责任不能单纯归咎于云平台服务商。而在实名备案方面，存在云平台服务商未落实用户身份信息登记和网站备案相关要求，导致虚假备案而被责任整改的案例。但如针对用户使用 PS 营业执照或印章、套用同名法定代表人身份证件等现象，现有审查方法无法有效发现和解决。一方面，云平台服务商在人工审核有效鉴别其身份真伪方面存在缺陷；另一方面，当前权威数据库仅比对营业执照上的证件号和单位名称，这种审核机制或导致缺乏主体真实信息而难以有效溯源，从而引发相应的安全责任。可以说，此类问题的安全责任界定仍存在模糊现象。

## 2. 应用安全责任

当前，国内的法律法规和政策对云平台的应用安全做出明确责任界定相对较少。《网络安全法》第十条、第二十七条，《电信条例》第五十七条，《电信业务经营许可管理办法》（工业和信息化部第 42 号令）第二十四条等，主要对云平台应用中可能存在的违规手段和目的做出规定。因此，云平台服务商和用户须做好自身业务应用系统在设计、开发、发布及配置等过程中的安全措施，承担相应的安全责任。

法规明确指出，作为增值电信业务经营者云平台服务商不得为未依法取得经营许可证或者履行非经营性互联网信息服务备案手续的单位或者个人提供接入或者代收费等服务。由此，云平台服务商需要履行对用户接入目的核实与监测义务，如若发现用户在云平台服务器上非法部署虚拟专用网络等应用，应当立即停止接入等服务，保存有关记录，并向国家有关机关报告。但在实际运行过程中，云平台服务商对云服务用户使用目的的全面核实仍无法实现，如对带登录态的网站存在技术难题。

### 3. 数据安全责任

数据安全责任是当前云平台服务商和用户最为关注的责任之一。《网络安全法》第二十一条、第三十七条，《全国人民代表大会常务委员会关于加强网络信息保护的决定》，《信息安全技术 云计算服务安全指南》（GB/T 31167-2014），《互联网信息服务安全管理系统使用及运行维护管理办法（试行）》第九条、第十三条、第十四条，《关于加强党政部门云计算服务网络安全管理的意见》，《云服务协助调查取证安全管理要求》第八条、第九条、第十条、第十一条、第十二条、第十三条等，对云平台数据安全责任做出了相关规定。其中，云平台服务商应承担监测与记录网络运行状态、日志留存、数据分类、重要数据备份、数据跨境与本地化留存、协助调查取证、将安全风险主动报告至主管部门等安全责任，用户则需承担部署或迁移到云计算平台上的数据和业务的最终安全责任。

但在云平台日常运行中，仍然存在责任无法明确落实的情况，云平台与用户之间的数据权限边界亟待厘清。在日志留存方面，云平台服务商可接触、管理和控制的数据主要是系统日志信息，实现技术功能、提高服务质量、维护客户数据和系统安全及遵照法律法规相关规定。若云平台某服务器上涉嫌内容违规，用户收到通报处置后可能会以后台登录等方式修改、删除数据，待后续监管部门调证时，服务器已不具备原始调证环境，云平台则被质疑“日志留存不全”，相应的安全责任无法有效落实。而针对数据跨境流动，我国规定云平台服务商收集和产生的个人信息及重要数据应当在境内存储，现有的《个人信息出境安全评估办法（草案）》等法规未正式出台，加之国际社会对云服务中的跨境数据存储、流动等监管尚未达成一致，这在一定程度上加大了云平台安全责任界定的难度。

### 4. 内容安全责任

内容安全责任的界定是国内云平台服务商和用户责任划分的难点。《网络安全法》第十二条、第二十八条、第四十七条、第四十九条，《全国人民代表大会常务委员会关于加强网络信息保护的决定》，《电信条例》第五十六条、第六十一条、第六十二条、第六十五条，《计算机信息网络国际联网安全保护管理办法》（公安部第33号令）第八条、第十条，

《公安机关互联网安全监督检查规定》（公安部令第 151 号）第十条，《非经营性互联网信息服务备案管理办法（试行）

》第十九条，《侵权责任法》第三十六条等法律法规涉及相关责任要求。用户需要承担保障内容安全的责任，云平台服务商不仅需要保障用户的数据与信息保密安全，还要承担内容安全巡查、违法违规内容处置、安全风险报告、执法协助等安全责任，若未采取法律规定的合理且必要的措施的，可能需要与该用户承担连带责任。

但在实践中，云平台服务商的主动巡查往往涉及权利与义务的对等性、用户隐私与商业秘密保护等问题，云平台安全责任的问题与矛盾集中凸显。

在违规和不良信息方面，监管部门要求云服务商重点加强对公开网站内容可能涉及的违法违规信息的巡查监测。其中存在的较为突出的问题为：一是对于云平台用户储存在云端的加密文件，云平台服务商往往处于保护用户隐私与解析内容监测的两难境地；二是对于带登录态功能的网站页面诱导点击进而推广宣传违法违规虚拟专用网络服务及其他不良信息的情况，云平台服务商往往因登录页本身不存在违法违规信息而难以进行有害内容巡查。对于上述问题的责任边界问题，业界尚未形成一致共识，但也有云平台服务商通过技术和商业模式创新，为云平台用户提供可靠的内容安全产品服务。

在知识产权侵权处置方面，与其他网络平台不同，云平台服务商作为底层技术架构和存储空间的提供者，不具有事先审查被租用的服务器中存储内容是否侵权的义务，也没有审查被租用的服务器存储内容是否侵权的权利，这与“故意视而不见等于明知”不同，云平台服务商并没有“故意忽视”侵权行为，其已满足了“红旗原则”下对网络服务商注意义务的要求。

<sup>[3]</sup>加之在云环境下权利人难以发现侵权行为，因此，云平台服务商无法实施《信息网络传播权保护条例》和《侵权责任法》第三十六条规定的针对具体侵权内容的“删除、屏蔽、断开链接”等必要措施，在法律层面应参照《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第四条，不主张云平台服务商构成侵权。

这并不意味着云平台服务商不承担侵权关系下的安全责任。一是在执法部门判断云平台用户侵权后，云平台服务商需要承担法律规定的配合处置的相关责任；二是在收到权利人侵权投诉举报的情况下，云平台服务商需视具体情况，履行和其商业模式风险相适应的注意义务，采取必要的、合理的、适当的措施配合权利人维权行为（见表 2）。

| 表 2 云平台安全的主体责任界定与难点 |             |       |        |
|---------------------|-------------|-------|--------|
| 安全域责任               | 国内法律法规的责任界定 |       | 待明确的问题 |
|                     | 云平台服务商      | 云平台用户 |        |
| 系统安全责任              | 网络安全防护、网站   | 实名备案等 |        |

|  |                   |  |  |
|--|-------------------|--|--|
|  | /App 实名备案、安全风险报告等 |  |  |
|--|-------------------|--|--|

|        |                                                        |                           |                                         |
|--------|--------------------------------------------------------|---------------------------|-----------------------------------------|
|        |                                                        |                           | 用户消极防护的安全责任界定，因技术等原因无法有效进行实名认证的安全责任等    |
| 应用安全责任 | 应用系统安全保障、用户应用目的核实与违规监测、安全风险报告等                         | 应用部署的合规与安全等               | 因技术等原因无法全面核实用户应用目的而带来的安全责任等             |
| 数据安全责任 | 监测与记录网络运行状态、日志留存、数据分类、重要数据备份、数据跨境与本地化留存、协助调查取证、安全风险报告等 | 部署或迁移到云计算平台上的数据和业务的最终安全责任 | 因交叉执法等原因可能存在责任无法明确落实，各国数据跨境要求差异带来的安全责任等 |
| 内容安全责任 | 保障用户的数据与信息保密安全，承担内容安全巡查、违法违规内容处置、安全风险报告、执法协助等责任        | 保障内容安全和合规                 | 因用户内容违规和不良信息与知识产权侵权等原因而形成的侵权连带责任        |



Excel 下载

表 2 云平台安全的主体责任界定与难点

（三）国外对云平台安全责任的主要监管思路与方式

1. 美国：基于安全评估与服务明确主体责任

对网络平台的治理，《美国通信法案》构建了独立的网络平台责任基本准则，特别是其中的第 230 条规定的免责条款及其适用范围，且在第 230

条立法时，美国国会明确宣称其立法的目的在于避免网络服务提供者背负对内容提供者发布的信息审查义务。美国的《数字千年版权法案》第 512 条第（m）条也规定，不得将有关网络服务提供者的法律责任或免责条款解释为网络服务提供者对于用户发布的网络信息负有监控或审查的义务。而美国联邦第二巡回法院在 BMG 和 EMI 案中确认了网络服务提供者对于重复侵权行为负有积极采取防范措施的义务。<sup>[4]</sup>在云平台监管方面，美国政府以第三方评估机构做支撑，对云服务进行安全评估，通过初始安全授权，加强双层授权机制，<sup>[5]</sup>同时对云平台服务商持续监管，注重对云平台和用户的自律引导，保证云服务的系统安全。

2011 年，美国预算管理办公室（OMB）发布《云计算环境下信息系统的安全授权》，即 FedRAMP 备忘录，建立了联邦政府风险授权管理项目，提供了采用云计算服务的低开销、高效率 and 基于风险的方法。<sup>[6]</sup>FedRAMP 规定，云平台服务商的相关安全责任有：①基于 FedRAMP 安全基线实施安全控制措施；②创建与 FedRAMP 需求一致的安全评估包；③与独立的第三方评估机构签订合同实施初始系统评估并要求持续评估和授权；④维护持续评估项目；⑤遵从有关变更管理和安全事件报告的要求。

与此同时，美国政府提供服务等级协议（SLA）、合同等指导，在标准模板中确立安全责任。2010 年 9 月发布的《政府客户云计算 SLA 考虑》，对政府部门与云平台服务商之间的 SLA 设计给出了具体的指南，涵盖 SLA 设计的背景、服务描述、测量与关键性能指标、连续性 or 业务中断、安全管理、角色与责任、支付与赔偿及奖励、术语与条件、报告指南与需求、服务管理、定义/术语表<sup>[7]</sup>等方面的内容与具体指导。在合同方面，2012 年 2 月发布的《联邦政府制定有效的云计算合同——获取 IT 即服务的最佳实践》给出了采购云服务的合同需求和建议，包括服务协议条款、保密协议、服务级别协议等，并分析安全、隐私、电子发现、信息自由访问、联邦记录保留等方面的需求，同时给出了具体建议。<sup>[8]</sup>

2017 年发布的美国《增强联邦政府网络与关键基础设施网络安全》行政令强调，政府执行部门和机构的负责人有责任管理其业务的风险，而且这种责任不能通过服务水平协议外包。这种权责分配思路在 2018 年更新版“联邦政府云战略”（Cloud Smart）中有所延续，即获取云服务的一个重要因素是明确云平台服务商能够执行什么服务以及在什么级别上执行什么服务，这将有助于机构确保有效、高效和安全地执行服务。<sup>[9]</sup>

2018 年 8 月，美国国家安全局在一份文件中提出了云平台安全责任应取决于用户选择的云服务与托管方式，并提出了国防部采购云服务应共享责任（见图 5）。云平台服务商和国防部共享独特且重叠的职责，以确保存储在公有

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/038053066034006127>