CSTC中国评测 见证质量 技术白皮书

电信和互联网行业数据安全治理白皮书（2020 年）

中国软件评测中心·网络空间安全测评工程技术中心

2020 年 7 月

序　言

世界主要国家纷纷采取数据本地化等强制性措施，维护数据主权并争夺数据资源。国内诸多政策、立法齐头并进，为推动数据安全及其治理实践提供全面保障，数据安全治理政策法律环境空前向好。

电信和互联网行业是全球数字化进程的先驱，随着行业数据内外部应用的同步拓展和推进，新技术新网络形态的创新融合应用，数据安全面临诸多新挑战，行业数据资源价值释放严重受阻，治理思路、治理模式、治理手段亟需创新。

本白皮书由中国软件评测中心网络空间安全测评工程技术中心撰写，参与人员包括白利芳、朱信铭、王涛、王翔宇、张嘉欢、张德馨、黄峥、宁黄江、李松恬，在此特别感谢中国电子信息产业发展研究院副院长黄子河、副总工程师安晖、中国软件评测中心副主任吴志刚及总工程师陈渌萍对本白皮书的撰写指导，感谢王芳、王闯两位同事研提的宝贵意见，及品牌宣传推广部刘喜喜、闫晓丽的编辑及排版支持，限于研究时间有限，报告内容难免存在纰漏，不足之处恳请各方同仁批评指正！

中国软件评测中心　唐刚

2020 年 7 月 3 日

版权声明

指导组：黄子河　安　晖　吴志刚　陈渌萍
编写组：唐　刚　白利芳　朱信铭　王　涛
王翔宇　张嘉欢　张德馨　黄　峥
宁黄江　李柲恬

目 录

前　言

网络信息技术创新日新月异，数字化、网络化、智能化融合发展，对我国建设网络强国、数字中国、智慧社会发挥着至关重要的作用。世界各国都把推进经济数字化作为创新发展的重要动能，并作出前瞻性布局。以数据为关键要素的数字经济发展历程中，数据价值也由最初的数据资源发展成为数据资产，再进一步发展为数据资本。4 月 9 日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，要求“加快培养数据要素”，将数据作为新型生产要素，正式与土地、劳动力、资本、技术等传统生产要素并列为国家基础战略性资源和社会生产创新要素之一。

电信和互联网行业（以下简称“行业”）在数据规模、覆盖范围、存储和传输能力，及实时性和多样性方面均具有突出的价值优势。随着行业数据内外部应用的同步拓展和推进，数据安全问题日益凸显，严重阻碍行业数据资源价值释放。做好行业数据安全治理刻不容缓。

本白皮书聚焦行业数据安全治理，首先，对数据治理、数据安全治理的内涵，以及行业数据主要分类、典型应用、安全发展形势进行了简要阐述和分析；其次，在梳理国内外数据安全治理环境的基础上提出行业数据安全治理需求，介绍了国内外数据安全治理的典型实践案例，并进行了问题分析；最后，提出行业数据安全治理框架和行业数据安全治理相关建议。

中国软件评测中心（工业和信息化部软件与集成电路促进中

心），简称中国软件评测中心，是直属于工业和信息化部的一类科研事业单位。长期服务和支撑国家部委、地方政府以及电信和互联网、交通、能源、银行、证券、保险、教育、卫生、广电、航空等各大行业，业务范围覆盖全国 31 个省、自治区、直辖市，业务网络覆盖全国 500 多个城市，构建了基于第三方服务的科技产业链。

网络空间安全测评工程技术中心（以下简称“网安中心”）是中国软件评测中心核心业务板块，致力于信息系统的网络安全防护和安全运行，支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，主营信息安全风险评估、网络安全等级保护测评、关键信息基础设施保护评估、数据安全能力和合规性评估等网络信息安全相关业务。

一、概述

(一) 概念及内涵

1. 数据治理概念分析

数据治理是近年来学术界、产业界关注的新热点，但关于数据治理这一概念的定义尚未完全统一。国际标准化组织、国际数据管理协会等国内外专业组织和部分知名研究机构都提出了其理解。

■ 国际标准化组织的IT服务管理与IT治理分技术委员会（ISO/IEC JTC1/SC40，简称SC40）关于数据治理的概念建立在IT治理的基础上，将ISO/IEC 38500的IT治理框架和模型应用于数据治理，认为数据治理为IT治理的一个子集或子域，通过持续的评价、指导和监督，平衡数据技术及其流程中的风险和收益，实现企业治理目标。即认为数据治理是数据在产生价值的过程中，治理主体对其进行评估、指导和监督的活动集合。

■ 国际数据管理协会（DAMA）关于数据治理的概念建立在数据管理的基础上，认为数据治理是数据管理的核心，是对数据资产行使权力和控制的活动集合(包括计划、监控和执行)，指导所有其他数据管理功能的执行，在更高层次执行数据管理。

■ 国际数据治理研究所（DGI）认为，数据治理和数据管理是两个完全独立的概念，并将数据治理定义为对数据相关事项作出决策和行使职权的活动，具体定义为一套信息相关过程的决策与问责体系，根据商定的模型执行，这些模型描述了谁可以根

据什么信息，在什么时间和情况下，用什么方法，可采取什么样的行动。

■ 国际知名 IT 咨询与研究机构 Gartner 与 DGI 有着类似定义，认为数据治理是一套决策权规范和问责框架，以确保数据和分析在评估、创建、使用及控制过程中的适当行为。

■ IBM 数据治理委员会认为数据治理是对企业中数据可用性、相关性、完整性和安全性的整体管理，以帮助企业管理其信息知识并理解数据。

■ 我国信息技术服务标准（ITSS）体系中的《信息技术服务 治理 第 5 部分: 数据治理规范》（以下称《数据治理规范》）中，将数据治理定义为数据资源及其应用过程中相关管控活动、绩效和风险管理的集合。

■ 《GB/T 35295-2017 信息技术 大数据 术语》和《GB/T 36073-2018 数据管理能力成熟度评估模型》中，将数据治理定义为数据进行处置、格式化和规范化的过程。是数据和数据系统管理的基本要素，涉及数据全生存周期管理，无论是出于静态、动态、未完成状态还是交易状态。

■ 中国银行保险监督管理委员会发布的《银行业金融机构数据治理指引》明确，（行业内的）数据治理是指银行业金融机构通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。

中国软件评测中心网安中心综合研究分析发现，与国外数据

治理大多率先在企业层面成功实践不同，国内对数据治理的研究更多站位国家治理、公共管理，再逐步形成规范指导组织（或企业）开展相关治理活动，即数据不仅仅是组织（或企业）的资产，更是国家的一种基础战略资源；数据治理主体不仅仅局限于企业，政府、市场、社会及个人也是重要主体，且治理实践不仅要依靠框架、模型和技术，还应结合政策、法律、教育、道德伦理等方法和手段，包括治理主体之间的统筹协调；数据治理目的不仅仅是确保数据的高效合理利用及企业的价值实现，更是为了提升国家治理能力和政府公共管理能力，即数据治理是国家治理体系和治理能力现代化的重要组成部分，影响着经济调节、市场经济、社会管理、公共服务等多个领域，关联着人才、资本、知识等各类要素，是一项系统性工作。

由此，本白皮书认为，**数据治理是多元治理主体以数据生产要素为对象，以释放数据价值为目标，以守住数据安全为底线，以建立健全数据全生命周期秩序规则为核心，以推动数据有序管理和流转为主要活动，以强化数据管理技术手段为支撑的一系列活动，具有综合性、复杂性和长期性等特征。**

2. 数据安全治理理念

数据安全治理的理念最早由 Gartner 正式提出，认为数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。组织内的各个层级之间需要对数据安全治理的目标和宗旨取得共识，确保采取合理和适当的措施，以最有效的方

式保护信息资源。微软则提出专门强调隐私、保密和合规的数据安全治理框架（DGPC），以更好实现数据安全风险控制。其数据安全治理理念主要围绕“人员、流程、技术”三个核心能力领域的具体控制要求展开，与现有安全框架体系或标准协同合作以实现治理目标。国内数据安全治理委员会认为，数据安全治理是以“让数据使用更安全”为目的，通过组织构建、规范制定、技术支撑等要素共同完成的数据安全建设的方法论。

总体而言，**数据安全治理是数据治理的一个重要组成部分，贯穿数据治理各个过程及数据全生命周期，聚焦数据的“安全”属性**，而数据治理则强调数据的“价值”属性。随着国际数据安全形势日益严峻，数据价值的释放严重受阻，数据安全治理迫在眉睫。电信和互联网行业数据资源丰富，对我国数据要素市场的培育具有不可替代的作用，为了保障行业数据资源价值的充分释放，行业应通力协作、主动出击，率先取得行业数据安全治理实践成功。

(二) 行业数据主要分类

1. 基于行业特点划分

行业基础网络数据。主要指用户及企业在使用电信基础网络设施过程中所产生的基础数据，包括了个人及设备的标识数据、位置及行为的日志数据等，依据对电信基础网络的调研结果，可以将其主要划分为:

- 基础信息类数据;
- 日志类数据;
- 结果类数据;

■ 辅助类数据;

■ 管理类数据。

行业基础业务数据。行业的数据资产结构主要与其开展的业务相关，目前较突出的是社交数据、电商数据、游戏数据、用户行为数据。其中:

■ 社交数据主要包括关系链数据、用户间的互动数据、用户自己产生的图文和视频内容、用户的位置信息等;

■ 游戏数据主要包括大型网游数据、网页游戏数据、手机游戏数据，及游戏活跃行为数据和付费行为数据;

■ 电商数据主要包括商品浏览、搜索、点击、收藏、购买、物流等数据;

■ 用户行为数据主要包括社交行为数据、访问浏览数据、搜索数据、消费数据等。

2. 基于服务对象划分

用户数据。各系统和业务的用户所拥有和产生的数据，主要包括了用户身份相关数据、用户服务内容数据、用户服务衍生数据等。

■ 用户身份数据主要包括了用户自然人身份标识和证明或网络虚拟身份标识、用户基本资料及私密资料等信息，以及用网络身份鉴权信息;

■ 用户服务内容数据主要包括了对用户提供的电信和互联网服务的内容数据、联系人信息等资料数据;

■ 用户服务衍生数据主要包括了服务订购数据、行为数

据、位置数据、征信或违规数据等用户衍生数据以及用户设备信息等数据。

企业运营管理数据。系统运行和业务流程中，服务于企业自身经营的各类数据，主要包括企业管理数据、业务运营数据、网络运维数据、合作伙伴数据等。

■ 企业管理数据主要包括企业内部管理数据，如发展战略及规划数据、财务数据、人事数据、对外合作数据及其他管理数据;

■ 市场经营类数据，如经营分析类数据、经营考核类数据、资源部署数据、营销方案等;

■ 企业公开披露和上报数据，主要指资本市场及主管部门要求公开或上报的数据;

■ 业务运营数据主要包括资费信息及管理信息、渠道数据、客服数据、营销数据及日常运营产生的其他数据等;

■ 网络运维数据主要包括密码及关联数据、资产资源类数据、支撑类数据等;

■ 合作伙伴数据包括合作伙伴基础资料信息、合同协议、合作过程中产生的数据等。

(三) 行业数据典型应用

1. 行业数据主要应用类型

行业基础网络应用。行业基础网络设施承载了几乎全行业的上层服务应用，基础设施规模及其承载的服务应用数据规模庞大，通过调研，行业基础网络数据的典型应用主要包括:

■ IDC/ISP 信息安全管理系统;

■ IP 资源管理系统;

■ 网络安全监测与管理系统;

■ 工业互联网安全监测系统;

■ 移动互联网综合监控平台以及反诈分析类系统等。

行业基础服务应用。行业基础服务应用主要是各个服务商应用其用户数据和企业经营管理数据进行分析，指导其自身经营活动或为用户/客户提供分析服务的各类应用。从自下而上可划分为七个层次的应用类型:

■ 数据基础平台层应用主要实现数据的有效存储、计算和质量管理;

■ 业务运营监控层应用主要是搭建业务运营的关键数据体系，在此基础上通过智能化模型开发出来的数据产品，监控关键数据的异动，通过各种分析模型等可以快速定位数据异动的原因，辅助运营决策;

■ 用户／客户体验优化层应用主要是通过数据来监控和优化用户／客户的体验问题;

■ 精细化运营和营销层应用主要通过数据驱动业务精细化运营和营销;

■ 数据对外服务和市场传播层应用一般服务于互联网企业的客户或用户，主要通过数据信息图谱和数据可视化产品来为客户提供数据分析服务;

■ 经营分析层应用主要通过分析师对大数据进行统计，形成经验分析周报、月报和季度报告等，对用户经营情况、收入

完成情况进行分析，发现问题，优化经营策略;

■ 战略分析层应用则既要结合内部的大数据形成决策层的数据视图，也要结合外部数据尤其是各种竞争情报监控数据、国外趋势研究数据来辅助决策层进行战略分析。

2. 行业数据典型应用案例

（一）典型商业应用

基于用户社交数据、行为数据和轨迹（LBS 定位）数据等进行用户画像，决策推送的广告类型，并对匹配的多家广告主提出竞价范围，经过各广告主竞价，最终将确定的广告内容推送至用户端，短短的 200 毫秒左右即可实现大范围的高速匹配和决策，实现精准营销。“大数据杀熟”也是利用了类似技术，包括数字版权、在线内容付费等领域也在借此辅助其更精准的将最匹配的内容和定价推送至每一个独特的用户个体。

电商平台在为用户提供商品的关键字索引服务时，搜索引擎对大量用户数据、商品数据、交易数据等数据资源进行文本分析、机器学习和同义词挖掘等，使得列出的商品更加满足客户的个性化需求并最终导致用户的购买行为。零售巨头沃尔玛借助语义搜索技术自行设计的搜索引擎 Polaris，使其在线购物完成率提升 10%到 15%。

（二）典型支撑应用

通过对话单数据、短消息、网络行为数据等数据进行识别、定位、拦截、统计分析和综合研判等，为主管部门及其他管理部门的反电信诈骗和互联网诈骗工作提供有力支撑。

借助复杂的大数据分析系统，通过对基础网络信令及日志数据、网站及 APP 应用的各类数据，进行实时感知预警、统计分析、综合研判、应急处置等，更好地支撑行业主管部门及其他执法部门开展网络舆情分析、社情民意调查、安全态势感知等工作。

由于行业基础网络设施、基础网络服务等优势，决定了其所承载数据类型的全面性，为政府其他工作的开展也起到不可替代的作用，如通过定位数据、用户通信数据、用户行为数据等指导防疫救灾、缓解交通拥堵、推动旅游业发展、提高公共设施维护效率等。

二、电信和互联网行业数据安全发展形势

(一) 行业数据安全总体形势

1. 事件影响范围不断扩大

电信和互联网行业是全球数字化进程的先驱。随着数字化进程的迅猛推进，数字技术已向行业全方位加速渗透、融合。数字化程度愈高，数据安全风险暴露面、攻击面越广，加之数据价值的提升，数据市场的驱动，数据利益相关方趋之若鹜，围绕网络攻击、数据窃取和数据交易形成的数据黑市已经成为大规模、有组织的犯罪集团，数据黑灰产猖獗，数据滥用及数据安全事件愈演愈烈。

2020 年 5 月 19 日，美国电信巨头 Verizon 公司发布 2020 年数据泄露调查报告(DBIR)。报告显示，81 个国家参与调研的数

据泄露事件中，55%的泄露事件和有组织犯罪相关，外部攻击占70%，企业内部攻击占 30%；58%涉及个人数据泄露，72%的受害者为大型企业。

从数据安全影响的对象来看，影响范围从最初的企业和个人逐步向整个行业及全社会蔓延。从发展的角度来看，首先，影响行业数据合理开放共享的意愿和积极性；其次，影响用户对行业数据安全治理的信心，从而影响行业新技术新业务与实体经济的深度融合；再者，数据安全问题为数据跨境流通、数据驻留规管带来负面影响，甚至面临被动局面。

2. 风险危害程度日趋严重

行业数据价值巨大，一旦出现安全问题，首先，会造成企业声誉和经济损失个人造成巨大的经济损失。2020 年 2 月 23 日，某 SaaS 服务商因员工恶意破坏公司线上生产环境及数据，导致其相关系统崩溃，大量商家的线上生意停摆，直至 3 月 3 日才完成了全部的数据恢复上线。此次事件后果严重，其服务的 300 万商户业务受到影响，在正式公告发出前 5 个工作日，股价下跌超 22%，股价缩水超 30 亿港元。据 IBM《2019 年全球数据泄露成本报告》显示，过去 5 年数据泄露成本上升了 12%，平均成本已达到 392 万美元。恶意数据泄露平均会给企业带来 445 万美元的损失，比系统故障和人为错误等意外原因导致的数据泄露高出 100 多万美元。

其次，可能危害到用户的生命或财产安全。如个人信息泄露不只是隐私权被侵犯的问题，也可能被犯罪分子利用，进行违法

犯罪活动，电信和互联网诈骗事件就是典型，也不乏个人信息泄露有关的命案。

此外，各国非常重视大数据在国家安全领域的运用，随着各国的数据战略部署，数据治理逐步上升到国家战略层面，某些数据安全事件极有可能发展为影响社会秩序、政治稳定、国家安全的非常事件。

3. 安全治理难度持续升级

引发数据安全风险的风险源可能是机器故障、内部人员的恶意行为或失误操作，也可能是外部黑客的恶意攻击；而恶意攻击途径又有不同，可能采用恶意软件、安全漏洞、社会工程学等手段或多种手段的组合；发起数据安全攻击的动机也不尽相同，单纯的炫技、商业或经济利益、军事或政治利益等。这为数据安全风险的防范带来一定难度。

此外，随着行业网络形态不断演化，新技术新应用场景的日渐复杂，衍生出新的数据类型、数据生产方式、数据处理方式和终端形式等，引发了新一轮的数据安全事件爆发，而对于新型安全风险的研究和防范能力目前还有待提升，安全挑战不断加剧。

再者，数字化的加速推进促进了复杂网络中的数据流，极大的模糊了传统数据安全的边界，使得行业基于边界或网元的防护体系不再能满足当前跨组织的数据流通安全风险管理、联动规范的接口管控、风险管控追踪等数据安全治理需求。多方面因素导致数据安全治理难度持续升级。

(二) 行业数据安全主要风险

1. 互联网暴露面问题突出

近年来，中国软件评测中心网安中心持续支撑工信部等监管机构开展对电信和互联网行业的威胁监测和远程检测，发现的安全漏洞或问题 80%和数据安全相关，主要包括 SQL 注入、非授权访问、数据泄露三大类。其中实现非授权访问的原因多样，包括弱口令、授权绕过、未进行身份验证等。数据泄露方面甚至存在源代码泄露。

2. 数据不可控性明显增加

随着信息技术的不断发展和信息化的不断普及渗透，行业数据产出以几何级增加，大数据中心和大数据系统应运而生。海量数据的生产、汇聚、存储、提炼、挖掘、应用等数据流转处理环节和流程大大增加。另一方面，就目前我国大数据技术架构而言，多数使用 Hadoop、Spark、MongoDB 等开源软件搭建平台，存在数据安全不可控的风险。此外，越来越普及的云计算，具有数据所有权和管理权分离的特点，用户对被存储在云端的数据是否完整无误，受到损坏后是否可恢复，是否被滥用，以及数据的存储策略、保留的副本数量、存储位置、销毁执行是否均按照 SLA 协议执行等均不可控。

3. 数据安全管理体系不完善

行业数据泄露事件时有发生，大多是事后发现和弥补，缺乏事前防范管理。主要表现在数据安全管理体系不健全，组织架构不完善、制度缺失、人员不足、意识不强、缺乏预案等方面。综

合中国软件评测中心网安中心多年的数据安全检查和评估项目实施等经验，行业在数据安全管理方面典型问题主要有:

■ 缺乏数据安全方面的管理机构。数据安全未引起足够的重视，未建立领导层面牵头的管理机构，数据安全管理责任无法明确和充分落实。

■ 数据安全控制措施不力。缺乏数据全生命周期安全管理相关规章制度，数据管理分散，未对数据资产摸底梳理，未合理配备相应的岗位和人员，数据未分级分类，没有严格的数据访问控制及权限管理，数据日志记录和审计措施不够，安全事件取证、分析、溯源能力不足，数据安全培训缺乏，应急预案不完善或缺失等。

■ 数据安全优先级不足。对数据安全风险的评估和认识不足，未将数据安全作为企业发展的重要考量，数据安全让步业务，系统带病运行。

■ 对数据安全合规性认识不足。缺乏数据安全合规性评估机制，不了解行业数据安全相关政策、法律法规、标准规范等，存在违规行为而不自知。

三、电信和互联网行业数据安全治理环境

(一) 国际数据安全治理环境

1. 欧盟密集立法深刻影响全球治理格局

欧盟“数据”和“安全”相关法律立法密集，与其“数字化单一市场”战略齐头并进，深刻影响国际数据治理格局，包括美国、

日本、韩国、印度、加拿大等在内的十几个国家为了打通欧盟立法产生的数据壁垒，与其已经达成或正在谈判以达成数据传输保护协议。其中，在美国曝光监听丑闻及棱镜事件后，欧盟认为欧美长达 15 年的《安全港协议》不足以保护欧盟公民隐私。2016 年 2 月 2 日，美国与欧盟达成新的隐私盾（EU-US Privacy Shield）协议，新协议要求美国企业履行更加严格的义务以保护欧盟公民的个人数据，并必须作出相应承诺。新协议实施不久便遭受阻碍，被法国多家隐私保护组织起诉至法院。2019 年 1 月 23 日，日本与欧盟达成数据共享协议，在欧盟对其进行充分性认定前，日本实施了额外的保障措施，以确保由欧盟转移的数据享有符合欧洲标准的保护保障，并进行至少每四年一次的协议运作审查。

表 1：欧盟近几年主要政策法律进展

年份	欧盟政策法律环境
2016	4 月 27 日，发布 2016/679 号条例《通用数据保护条例》（GDPR），条例制定了个人数据保护的一般规范，为欧盟内外个人数据的自由流动提供了确定性保护，开启了其成员国新一轮数据立法，是欧盟新形势下数据治理的里程碑事件。
	7 月 6 日，颁布首部网络安全相关法律《网络与信息系统安全指令》（NISD），旨在加强基础服务运营商、数字服务提供商的网络与信息系统安全，并要求成员国及时转化为国内立法，与 GDPR 分别从安全和基本权利保障两个层面实现其网络治理战略意图。
2018	10 月 23 日，发布 2018/1725 号条例《联盟机构个人数据处理保护条例》，作为 GDPR 的补充对欧盟机构处理个人数据时对自然人的保护提出基本要求，明确了数据主体的权利范围及主要监管机关的职能和义务。
	11 月 14 日，发布 2018/1807 号条例《非个人数据自由流动条例》，对数据本地化要求、主管当局的数据获取及跨境合作、专业用户的数据迁移等问题作了具体规定，并考虑了服务提供商负担过度及市场扭曲

年份	欧盟政策法律环境
	的问题，进一步完善了欧盟数据治理框架。
2019	4 月 17 日，颁布 2019/881 号条例《关于 ENISA 和信息通信技术网络安全认证的条例》（又称《2019 网络安全法案》），法案指定欧盟网络和信息安全署（ENISA）为永久性欧盟网络安全机构，确立了第一份欧盟范围的网络安全认证计划，以确保向欧盟境内提供的产品、流程和服务满足其网络安全标准。欧盟网络安全治理的里程碑事件。
	6 月 20 日，发布《数据开放指令》
2020	2 月 19 日，发布《欧盟数据战略》，从构建统一数据治理架构、加强数据基础设施建设、加大数据技能和素养投资、打造欧洲数据空间等方面概述了欧盟在数据方面的核心政策举措及未来 5 年数据投资战略。

数据来源：中国评测网安中心，2020 年 7 月

2. 美国多点立法捍卫其多元化社会利益

目前美国尚无联邦层面的综合性数据安全正式立法，但在联邦层面多次强调将数据作为执法优先项。受欧盟数据立法影响，2018 年 6 月 28 日，美国在州层面通过第一部数据隐私法案《加州消费者隐私法案》，随后提出《数据保护法案》，并于 2019 年底相继提交《国家安全和个人数据保护法提案》、《联邦数据战略与 2020 年行动计划》。此前，特朗普签署了《外国情报监视法案修正案》第 702 条的更新授权，同意授权美国国家安全局(NSA)监听境外目标人员并收集其相关数据情报。并签署《澄清合法使用海外数据法》即“CLOUD 法案”，根据该法案，无论美国网络服务提供商的数据是否存储在美国境内，只要是提供商拥有、控制或监管的数据，均须按照该法令的要求保存、备份和披露。同时允许“适格外国政府”执法机构调取美国存储数据，但“适

格”认定、调取规则以及上述域外数据采集要求均以美国利益为先加以制衡。

表 2 ： 美国政策法律环境

年份	美国政策法律环境
2018	1 月 11 日，通过《外国情报监视法案修正案》第 702 条的更新授权，延续其霸权形式的互联网监视及情报收集计划
	3 月 23 日，签署《澄清合法使用海外数据法》，提升了美国执法机构对境外存储数据的执法权限
	6 月 28 日，通过第一部数据隐私法案《加州消费者隐私法案》，强化了数据主体对个人信息的控制权,规范了企业收集处理数据的方式，于 2020 年 1 月 1 日正式生效
	12 月 13 日，提出《数据保护法案》
2019	11 月 18 日，提交《国家安全和个人数据保护法提案》
	12 月 23 日，发布《联邦数据战略与 2020 年行动计划》，以数据治理视角，描述了联邦政府 2020 年起的未来 10 年的数据愿景，并确定了 2020 年需采取的 20 项关键行动

数据来源：中国评测网安中心，2020 年 7 月

3. 国际数据治理情绪高涨配套动作频繁

2017 年至今，日本、澳大利亚、越南、巴西、加拿大、印度、新加坡等国家纷纷出台数据相关政策法律，其中，加拿大的《个人信息保护和电子文件法》修正案增加了强制性数据泄露通知报告要求。印度的《个人数据保护法案》，引入了更为广泛的数据本地化要求，对包括互联网行业在内的多个行业带来全面冲击。新加坡通信信息部和个人数据保护委员会联合发布的《个人数据保护法（修订）》草案，是规范个人数据的收集、使用和披露的综合性立法，为配合该法更好执行，还配套出台了特定领域

（如电信、房地产、教育、医疗、社会公益服务等行业）的个人数据保护指南。

此外，美国主导下的亚太隐私数据跨境体系（APEC CBPRs）也在沉寂期后迎来实质性进展。2018 年，新加坡、澳大利亚和中国台北获 APEC 批准，加入 CBPRs 体系。截至目前，在 APEC 21 个经济体中，已有包括美国、日本、加拿大、韩国、新加坡等 8 个经济体加入 CBPRs 体系。意味着体系内成员国的认证企业之间个人信息的跨境流动不受阻碍。ODCE 经合组织也在继 2013 年 7 月发布《隐私及个人数据跨境流动保护指引》后，于 2019 年 11 月，发布报告《公共部门如何实现数据驱动》，以促进公共部门采用更多数据驱动的方法来制定政策、提供服务，并提出关于建设数据驱动型公共部门的建议。

全球数据安全标准发展迅速，包括国际标准组织 ISO、国际电信联盟 ITU-T、全国信息安全标准化技术委员会（TC260）、以及互联网行业管理部门工信部下属行标数据安全组织 CCSA TC8 的相关数据安全标准及其体系。关于数据治理相关标准或框架目前的主流成果包括：国际标准化组织的数据治理国际标准（ISO/IEC 38505）、国际数据管理协会的数据管理知识体系指南（DAMA-DMBOK）、国际数据治理研究所（DGI）的数据治理框架、IBM 数据治理委员会的数据治理成熟度模型以及我国信息技术服务标准（ITSS）体系中的数据治理规范。

表 3：　其他国际组织政策法律环境

年份	国际其他组织政策法律环境
2017	5 月 30 日，日本《个人信息保护法》修订版全面实施

2018	2 月 22 日，澳大利亚隐私法修正案《数据泄露通知计划》正式实施
	6 月 12 日，越南通过《网络安全法》
	8 月 14 日，巴西批准《通用数据保护法》
	11 月 5 日，加拿大《个人信息保护和电子文件法》修正案生效
	新加坡、澳大利亚、中国台湾加入 APEC CBPRs 体系
2019	12 月 4 日，印度通过《个人数据保护法案》
	11 月 28 日，ODCE 经合组织发布报告《公共部门如何实现数据驱动》
2020	5 月 14 日，新加坡发布《个人数据保护法（修订）》草案

数据来源：中国评测网安中心，2020 年 7 月

(二) 国内数据安全治理环境

1. 国内政策多头并进迎来治理新格局

2015 年以来，国家出台多部重大立法，《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《中华人民共和国电子商务法》、《中华人民共和国密码法》、《中华人民共和国民法典》等多部法律颁布并施行，分别从不同角度不同程度地对个人信息和数据保护做了相关规定。

国务院先是于 2017 年印发《关于运用大数据加强对市场主体服务和监管的若干意见》，提出充分运用大数据先进理念、技术和资源，加强对市场主体的服务和监管，推进简政放权和政府职能转变，提高政府治理能力。又于 2020 年印发《关于构建更加完善的要素市场化配置体制机制的意见》，提出“加快培育数据市场要素”，优化经济治理基础数据库，培育数字经济新产业、新业态和新模式，加强数据资源整合和安全保护。

国家互联网信息办公室于 2019 年发布《数据安全管理办法

（征求意见稿）》，对利用网络开展数据收集、存储、传输、处理、使用等活动，以及数据安全的保护和监督管理，做了详细规定；并发布《个人信息出境安全评估办法(征求意见稿)》，目前两项公开征求意见工作均已完成。随后，审议通过《儿童个人信息网络保护规定》。

2020 年 1 月 17 日至 18 日，中央政法工作会议强调，要把大数据安全作为贯彻总体国家安全观的基础性工程，依法严厉打击侵犯公民隐私、损坏数据安全、窃取数据秘密等违法犯罪活动。此外，从 1980 年提议到被纳入十三届全国人大常委会立法规划的《电信法》，历时 39 年终于迎来新进展，同样被纳入规划的《个人信息保护法》和《数据安全法》已列入 2020 年立法工作计划，其中《个人信息保护法》已形成草案稿（尚未提请审议），《数据安全法（草案）》已于 2020 年 6 月 28 日提请十三届全国人大常委会第二十次会议审议。

国内诸多政策、立法齐头并进，为数据及其安全治理落地实践提供全面保障。总体来说，全球政策法律环境由前期的以信息自由、数据共享为价值导向，逐步发展到以个人信息及隐私保护为重点，而后向全面的数据治理扩张，为数据安全治理及其法治化提供了良好的政策环境保障。

表 4:　国内政策法律环境

年份	国内政策法律环境
2015	7 月 1 日，颁布《国家安全法》、印发《关于运用大数据加强对市场主体服务和监管的若干意见》
2017	6 月 1 日，《网络安全法》正式施行，对个人信息保护作出明确规定
2018	8 月 31 日，颁布《电子商务法》，除了对个人信息保护作出规定外，

年份	国内政策法律环境
	对于“数据杀熟”问题也首次尝试作出回应
2019	5 月 28 日，发布《数据安全管理办法（征求意见稿）》
	6 月 13 日，发布《个人信息出境安全评估办法(征求意见稿)》
	10 月 1 日，《儿童个人信息网络保护规定》正式实施
	《电信法》被纳入十三届全国人大常委会立法规划
2020	1 月 1 日，《中华人民共和国密码法》正式施行
	4 月 9 日，印发《关于构建更加完善的要素市场化配置体制机制的意见》
	4 月 27 日，12 部门联合发布《网络安全审查办法》，明确网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，包括网络产品和服务使用后带来的关键信息基础设施重要数据被窃取、泄露、毁损的风险
	5 月 28 日，通过《中华人民共和国民法典》，第六章“隐私权与个人信息保护”明确了隐私权、个人信息的定义，典型的隐私权侵害行为，个人信息处理的原则和条件，个人信息主体的权利，信息处理者的安全和保密义务等内容
	被列入 2020 年立法工作计划的《数据安全法》草案已于 6 月 28 日提请审议；《个人信息保护法》草案稿待提请

数据来源：中国评测网安中心，2020 年 7 月

2. 国内数据治理标准化进展领先国际

国内在数据治理标准化进展方面，处于主导地位。2014 年，ITSS 分委会启动了数据治理标准预研工作，并向 SC40/WG1 提交了《数据治理白皮书》（英文版）和数据治理研究技术报告，获得国际专家一致认可。2015 年 5 月，在巴西 SC40 全会上，中国代表团正式提出“数据治理国际标准”新工作项目建议并获通

过。会议决定将数据治理国际标准分为两个部分，其中，ISO/IEC 38505-1《ISO/IEC 38500 在数据治理中的应用》（以下称 ISO/IEC 38505-1）由中国国家成员体（SAC）申请立项并由我国专家作为联合编辑研制，并于 2017 年 3 月 31 日获得国际标准化组织批准，并正式发布，这是国际上第一个数据治理国际标准。第二个部分 ISO/IEC TR 38505-2《数据治理对数据管理的影响》（以下称 ISO/IECTR 38505-2）是由我国专家主导编辑研制的第二个数据治理领域的重要国际标准，并于 2018 年 5 月 16 日获批发布。项目期间，ITSS 分委会同步开展了数据治理国家标准的研制工作，并于 2018 年 6 月 7 日正式发布 GB/T 34960.5-2018《信息技术服务治理第 5 部分：数据治理规范》。

表 5 ： 国内主要标准化进展

年份	国内主要标准化进展
2014	向 SC40/WG1 提交了《数据治理白皮书》（英文版）和数据治理研究技术报告
2017	3 月 31 日，国际标准 ISO/IEC 38505-1：《信息技术-IT 治理-数据治理-第 1 部分：ISO/IEC 38500 在数据治理中的应用》正式发布
2018	5 月 16 日，国际标准 ISO/IEC TR 38505-2 获批发布
	6 月 7 日，发布 GB/T 34960.5-2018《信息技术服务治理第 5 部分：数据治理规范》

数据来源：中国评测网安中心，2020 年 7 月

四、电信和互联网行业数据安全治理需求

(一) 国内外政策形势紧迫

欧盟 GDPR 深刻影响全球数据治理生态，尤其是明确规定了

欧盟境外的主体在特定条件下也必须遵循 GDPR 相关规范。如GDPR 定义的处罚标准可能让企业面临“上限 2000 万欧元或全年营业额的 4%（取高者）”的罚款。在数字经济全球化的当下，迫使包括中国在内的治理主体在数据治理战略部署，及中国企业在内的跨境数据运营主体在业务合规过程中，必须考虑、评估 GDPR 的约束和实际影响力。2019 年 1 月，Google 由于其个性化广告推送服务中违反 GDPR 的透明性原则，且在处理用户信息前未获得有效同意，被罚 5000 万欧元。截止目前，依据 GDPR 全球共开出大约 300 张罚单，涉及金额约 35 亿欧元，被罚企业不乏德国宽带运营商 1&1、意大利电信运营商 TIM 等电信企业。

此外，美国、日本、韩国、加拿大、澳大利亚等发达国家和巴西、印度等发展中国家也在数据治理进程中表现出极大热情，在指导各自境内企业或组织保障个人信息和数据安全同时，均在全球化数字经济中尽可能最大化自身利益。此外，国内对“数据要素”的定位，及数据安全相关立法的滞后，也对数据安全治理提出要求和挑战。受国际及国内关于“数据”、“安全”及其他配套政策和立法形势影响，行业数据安全治理迫在眉睫。

(二) 安全和发展双重驱动

习近平总书记在 2016 年 4 月 19 日的网络安全和信息化工作座谈会上强调，安全是发展的前提，发展是安全的保障，安全和发展要同步推进。自 2020 年 3 月 4 日，中央政治局会议强调加快 5G 网络、数据中心等新兴基础设施建设以来，全国各地方政府纷纷公布新基建投资计划，为我国数字化增速转型提供了新动

能，行业发展也迎来新机遇，但同时也会面临新的安全风险，为避免因安全问题造成巨大的经济和社会损失，同步规划、建设数字新基建安全保障措施势在必行，其中，数据安全保障措施的规划和建设首当其冲。

网络信息时代，大数据、云计算、人工智能等新型技术，物联网、车联网、工业互联网等新形态网络，以及远程医疗、在线教育、直播新媒体等新型应用蓬勃发展，新技术新业务的安全管理、安全评估、安全测评等能力尚不成熟，行业数据安全面临更严峻的挑战，如大数据平台对外业务合作过程中的数据滥用问题，云环境下数据脱离了数据拥有者物理管控的问题及云服务商是否遵守云存储服务 SLA 协议的问题等，严重影响行业健康发展。

此外，数字经济飞速发展，数据价值催生了数据黑产，从黑客、内鬼非法盗取个人信息，到个人数据在互联网被公开兜售、暗网数据交易，再到电信互联网诈骗、企业精准营销“杀熟”、虚拟资产盗取等数据黑产及滥用乱象，反向刺激了行业数据安全的监管需求及治理思考。

(三) 数据拥有者权益期待

据中国互联网络信息中心 CNNIC 第 45 次《中国互联网络发展状况统计报告》，截至 2020 年 3 月，我国网民规模为 9.04 亿，互联网普及率达 64.5%。受疫情影响，网络应用的用户规模呈现较大幅度增长。其中，在线教育、在线政务、网络支付、网络视频、网络购物、即时通信、网络音乐、搜索引擎等应用的用户规

模较 2018 年底增长迅速，增幅均在 10%以上。坚实的用户基础推动了行业的蓬勃发展，同时也为行业带来新的挑战。

就疫情期间而言，包括个人姓名、身份证、手机号码、具体住址等大量实名信息被社区、酒店、餐饮业等组织或机构强制性收集，而多数数据收集者并不具备个人信息保护的意识和能力，个人数据权益无从保障，数据拥有者急切期待相应体系化措施更有力且正当化地保护其个人数据。

而日常情形下，公众依然希望企业或组织尊重个人隐私，数据拥有者依然期望数据掌控权不要脱离或失控，并期待提高采集和使用其数据的相关行为透明度。行业在发展和建设过程中，数据拥有者的权益衡量和基于行业的利益平衡需要给予更多关注，比如关于数据安全企业及用户各自明晰的权利和义务设定，关于数据拥有者权利合理的变现保障和便利的变现渠道以及严密的数据安全相关行为和事件的责任追究机制等。

五、电信和互联网行业数据安全治理实践

(一) 国外典型实践案例

1. 微软之 DGPC 框架

微软早在 2010 年 11 月，就从数据隐私合规角度提出针对隐私、保密和合规的数据治理（DGPC）框架，主要围绕人员、流程和技术三个核心能力维度领域展开。

人员能力维度: 微软认为数据治理流程和工具的有效性取决

于使用和管理它们的人员，所以框架首先围绕人员展开。建立一个由组织内部人员组成的 DGPC 团队，明确定义其角色和职责，提供足够的资源来执行他们所需的职责，以及对总体数据治理目标给予明确指导。并表明，该团队实质上是个虚拟组织，其成员共同负责定义对数据分类、保护、使用和管理过程中关键方面管理的原则、政策和过程。

流程能力维度: 梳理必须满足的各种要求涉及的各种权威文件(法律、法规、标准以及公司政策和战略文件)，并理解这些法定要求、组织策略和战略目标是如何相互交叉并影响的，有助于组织将其业务和遵从性数据需求(包括数据质量指标和业务规则)整合为一个协调的集合。而后定义满足这些需求的指导原则和策略。最后，确定在特定数据流程中数据安全、隐私和合规面临的威胁，分析相关风险并确定适当的控制目标和控制活动。

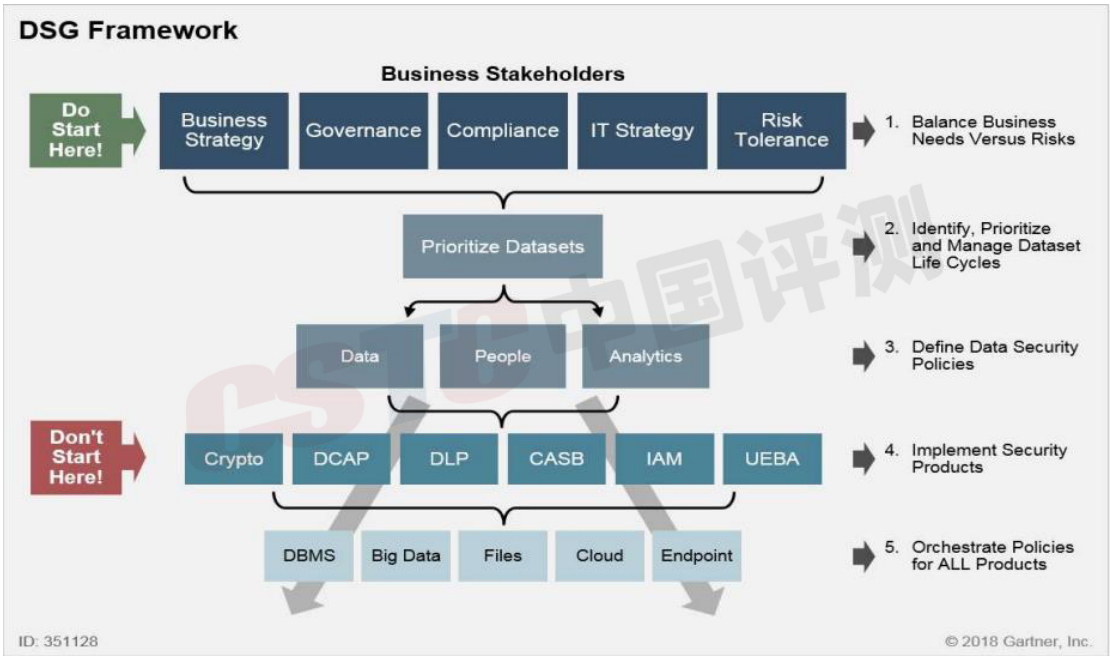
技术能力维度: 即微软开发的一种分析特定数据流的方法，以识别信息安全管理系统或控制框架更广泛的保护措施都可能无法解决的残留的、特定流的风险。这种方法包括完成一个称为风险/差距分析矩阵的表单，表单主要围绕三个元素构建:信息生命周期、四个技术领域以及组织的数据隐私和机密性原则。

2. Gartner 之 DSG 框架

全球领先的 IT 研究和咨询机构 Gartner 对数据安全治理进行了专项的研究和分析，于 2018 年 4 月正式推出数据安全治理（DSG）框架（见**错误!未找到引用源。**1），并提出安全和风险管理领导者应使用 DSG 框架来减轻由数据安全威胁、数据驻留

和隐私问题引起的业务风险。框架的基本思路是对全生命周期的数据集进行识别、分类和优先级排序，使用 CARTA 模型选择和明确与数据集优先级相匹配的数据安全策略规则和功能，随后部署安全产品、配置策略，并定期或在业务风险发生变化时检查安全策略规则和功能的适用性。

图 1：Gartner 数据安全治理（DSG）框架



图片来源：Gartner 官方网站，2018 年

具体对应到框架中，主要包括业务需求和风险平衡、优先数据集、策略制定、安全工具和策略配置五个层面，具体如下。

- 经营利益相关者在治理工作开战前应达成多方面的共识，包括经营策略、治理、合规、IT 策略和风险容忍度等方面；
- 对全生命周期的数据集进行识别、分类、分级；
- 在分类分级基础上，明确被保护的数据对象、数据涉及人员及其行为，而后基于此明确不同类别不同级别的被保护数据本身的全生命周期安全策略，以及相应人员及其行为

的安全管控策略等;

- 随后采用多种安全产品支撑安全策略的实施，包括加密系统、以数据为中心的审计和保护系统、数据防泄漏系统、云访问安全代理、身份识别与访问管理系统等;
- 最后为所有产品配置策略并保持策略下发同步，策略执行对象包括关系型数据库、大数据、文件、云、终端等。

(二) 国内典型实践案例

1. 监管层主要实践

行业数据安全专项治理。2019 年 1 月 25 日，中央网信办、工信部等四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，决定自当年 1 月至 12 月，在全国范围内组织开展 App 违法违规收集使用个人信息专项治理行动，并于年底印发《App 违法违规收集使用个人信息行为认定方法》。其中，工信部开展的“App 侵害用户权益专项整治行动”，对 236 款 App 运营者下发整改通知书，公开通报 56 款，下架 3 款。2019 年 7 月 1 日，工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，开展为期一年的专项行动，从完善网络数据安全制度标准、开展合规性评估和专项治理、强化行业网络数据安全管理、推动网络数据安全技术防护能力建设等方面综合推进，有力推动了行业数据安全治理体系构建。2020 年 5 月 14 日，工信部印发《关于 2020 年电信和互联网行业网络数据安全管理管理工作的通知》，明确开展行业数据安全和个人信息保护违法违规行为集中治理、APP 违法违规收集使用个人信息专项

治理、疫情防控中个人信息安全风险专项排查等相关工作部署。

行业数据安全合规性评估。2019 年，工信部部署全国基础电信企业（含专业公司）、50 余家重点互联网企业及 400 余款 APP 运营者，结合重点业务类型和场景，依托互联网新技术新业务安全评估机制，对标《2019 年基础电信企业数据安全合规性评估要点》和《2019 年互联网企业数据安全合规性评估指引》，全面开展网络数据安全合规性评估，并将其作为重点工作内容纳入年度网络信息安全“双随机一公开”检查和基础电信企业网络与信息安全责任考核检查。2020 年印发的《关于 2020 年电信和互联网行业网络数据安全管理管理工作的通知》中，明确行业开展网络数据安全合规性评估工作的相关部署，并发布《2020 年电信和互联网企业网络数据安全合规性评估要点》。

数据安全制度标准建设推进。加速推进行业数据安全指导意见的出台，以明确行业数据分类分级、安全评估、安全认证、预警处置等关键制度规范和要求。部署行业按照法律法规要求，健全完善企业内部网络数据全生命周期安全管理制度，并加快完善行业数据安全标准体系。2020 年 3 月 4 日，工信部印发《工业数据分类分级指南（试行）》，指导工业领域产品和服务全生命周期产生和应用的数据的分类分级工作。4 月 10 日，工信部公示《网络数据安全标准体系建设指南》（征求意见稿），提出“到 2021 年，初步建立网络数据安全标准体系”，“到 2023 年，健全完善网络数据安全标准体系”的建设目标。

行业数据安全监督执法。依据《网络安全法》《电信和互联网用户个人信息保护规定》等法律法规，委托第三方机构采取远

程检测、现场检查、专项检查等方式开展监督检查，其中，企业数据安全责任落实情况及合规性评估落实情况被作为重点内容，纳入网络信息安全“双随机一公开”检查和基础电信企业网络与信息安全责任考核检查。数据安全事件的监测跟踪和执法调查力度空前加大，对违法违规行为采取约谈、公开通报、行政处罚等措施，并将处罚结果纳入电信业务经营不良名单或失信名单。数据安全投诉、举报机制也在逐步改善。

2. 企业层实践案例

基础电信企业方面，以中国移动通信有限公司为例，针对大数据安全提出一套治理方案，主要围绕安全策略、安全管理、安全运营、安全技术、合规评测、服务支撑等六大保障体系，构建了大数据安全保障框架。其中：

- 安全策略体系，主要描述了公司在大数据安全管理方面的总体方针，是其它体系建设的基本依据；
- 安全管理体系，主要描述了大数据内部管理、第三方合作管理、数据分类分级等方面的安全要求和实施方法；
- 安全运营体系，主要描述了大数据业务运营部门在数据安全运营和业务安全运营过程中的要求和实施指南；
- 安全技术体系，主要描述了对大数据平台系统的安全防护要求、基线配置要求及实施指南；
- 安全评测体系，主要描述了开展大数据安全管理与技术评测方法、流程、指南；
- 服务支撑体系，主要描述大数据在安全领域的应用，特别

是在数据防泄漏、安全态势感知、不良信息治理方面的应用方法。

互联网企业方面，阿里云为了保障大数据分析平台和应用中用户数据的安全，在 2016 年 1 月发布的《数据安全白皮书》中构建了自己的数据安全体系，并提出了阿里云永远不动客户数据的“数据保护倡议书”。阿里云的数据安全体系从数据业务安全、数据产品安全、底层数据安全、云平台安全、接入和网络安全、运维管理安全等六个方面提供保障数据生命周期安全的技术和管理措施。在数据安全治理方面主要分为了治理层、管理层和技术层，其中：

- 治理层主要考虑了企业战略与组织保障、数据安全监管合规、SLA 等方面；
- 管理层主要是全生命周期的数据安全管理；
- 技术层主要包括资产管理、权限控制、监控审计和安全防护等方面。

天融信将数据安全治理的框架大致分为治理层、管理层和支撑层三个层面，其中：

- 治理层主要考虑了数据治理总目标、组织结构及授权、数据安全制度、数据安全流程等方面；
- 管理层主要是指数据安全管理文件体系；
- 支撑层主要是指数据安全综合管理系统，包括各类数据管理和数据安全防护涉及的子系统。

安全企业方面，安华金和认为数据安全治理是以“让数据使用更安全”为目的的安全体系构建的方法论，核心内容包括：

■ 三个主要需求目标，数据安全保护、合规性、敏感数据管理;

■ 三大核心理念，分级分类、角色授权、场景化安全;

■ 六个主要建设步骤，组织构建、资产梳理、策略制定、过程控制、行为稽核和持续改善;

■ 一个核心实现框架，框架内容包括数据安全人员组织、数据安全使用的策略和流程、数据安全技术支撑三大部分。

上海观安以数据流转生命周期为主线，以“平台安全、数据安全、运维安全、安全分析”为核心，提供以数据为中心而非以网元为中心的数据安全解决方案，其数据安全治理框架大致分为防护层、监控层、管理层，其中:

■ 防护层以安全技术应用、安全架构应用和安全防护系统作为主要支撑;

■ 监控层以安全分析平台和安全管理平台作为支撑;

■ 管理层主要聚焦安全运营管理和专业安全服务。

(三) 国内外实践对比

本节对国内外数据安全治理标志性实践进行对比，即关于“数据安全治理”概念、框架和方案正式提出、专项推进的里程碑性事件的实践进程对比。总体来说，国内外的数据安全治理标志性实践进程基本一致，详见图 2。

图 2：国内外标志性实践进程

图片来源：中国评测网安中心，2020 年 7 月

1. 国外标志性实践

2015 年，Gartner 提出数据安全治理的概念和相应的原则与框架。2017 年，Gartner 提出同样适用于数据安全评估与控制的持续自适应的安全风险和信任评估模型（CARTA），并在 Gartner 全球安全大会上，多位分析师在数据安全、安全治理的相关研究报告中，多次提及数据安全治理并加以强调，认为数据安全治理已成为了数据安全中的“风暴之眼”（The Eye Of Storm）。2018 年 3 月，Gartner 的分析师在研究报告中提出使用分类工具改善数据安全治理。4 月，推出研究报告《如何使用数据安全治理框架》，正式提出数据安全治理（DSG）框架，并预测到 2021 年，超过 31%的企业将实施数据安全治理架构，当时比例不足 5%。2019 年 12 月，Gartner 再次推出针对数据安全治理研究报告《使用数据安全治理框架平衡业务需求和风险》。 2020 年 4 月，在研究报告《如何在企业版 DLP 和集成版 DLP 方案之间进行选择》中，提出安全和风险管理者应借助 DSG 框架，在两种数据泄露

防护（DLP）方案之间做选择。

2. 国内标志性实践

2015 年，国内企业安华金和正式提出数据安全治理理念和框架。2017 年，中国网络安全产业联盟成立数据安全治理工作组并组织召开中国首届数据安全治理高峰论坛。2018 年，网络安全与信息化产业联盟在中国网信联盟的指导与支持下组织召开了第二届数据安全治理高峰论坛，并宣布成立全国首个数据安全领域的专项委员会——数据安全治理委员会，并发布《数据安全治理白皮书》。2019 年，国内《数据安全治理建设指南》及《数据安全治理白皮书 2.0》在第三届数据安全治理高峰论坛上发布。 此外，在 2019 世界人工智能安全高端对话上，赛博研究院和上海观安信息技术股份有限公司联合发布《人工智能数据安全风险与治理》报告，提出了人工智能数据安全治理的目标、框架及治理措施，以及有效解决人工智能中的数据安全问题的建议和思路。

(四) 行业实践问题分析

1. 企业顶层驱动力不足

行业目前的数据安全治理实践，在企业层面大多由单个部门（如 IT 部门或安全部门）主导驱动，缺乏高层的有效参与，顶层驱动不足。负责决策、管理、技术及监督的人员责权不明晰，问责机制不严密，大多数企业的数据安全工作聚焦在管理层和执行性，甚至只在执行层开展相关工作，在治理层进展很少，尚未形成安全治理体系。

2. “网元”模式待升级

行业数据释放价值的过程必然是其流动、共享、交易和使用的过程，数据滥用、数据泄露、数据确权等问题不可避免，目前以网络或系统单元为中心的安全防护模式，往往不能将数据的安全措施和安全需求精确匹配。例如由于数据要素的流动性、可复制性等特有属性，高敏感级别的数据可能流入或存储在比其敏感度低的网络或系统，直接影响数据安全治理效果。

3. 缺乏用户侧权益考量

默认勾选、霸王条款、未经授权的电信和互联网营销、电信和互联网诈骗等现象在日常生活中屡见不鲜，用户并没有实质的选择机会或权力，权益被侵害时缺乏便利且有效的渠道去维护，行业对用户数据权益的合理考量尚欠缺。

六、电信和互联网行业数据安全治理框架

中国软件评测中心网安中心综合上述分析，提出数据安全治理体系框架，框架主要由治理层、管理层、执行层和监督层四个层面组成，具体细节见图 3。

(一) 数据安全治理层

治理层主要活动包括数据安全治理体系的战略决策，组织职能架构设计，制度体系框架设计及治理流程体系设计等。**职能架构**与数据安全治理体系框架相匹配，主要由决策层、管理层、执行层和监督层四个逻辑层组成，分别承担体系决策、建设、执行

和监督的职能。组织架构基于职能架构配套设计，其中，决策职能层一般由数据安全归口管理部门或责任部门的高层管理者组成，管理职能层一般由责任部门的中高层管理人员组成，执行职能层由具体的业务部门、平台建设部门、运营维护部门、安全部门等系统或平台相关部门的技术人员和管理人员，以及人事、财务、保密等综合管理部门的相关人员组成，审计职能层主要以监管部门、审计部门或第三方评估机构为主，开展数据安全相关监督、审计和评价等事宜。**制度体系**是指企业为维护内部纪律和公共利益制定的，治理相关参与者遵守的政策规范、标准要求、实施指南、操作规程等。**流程体系**是指企业为了达到治理目标和效果，通过明确的标准的步骤执行并输出成果的系列管理流程，主要包括评价（评估）流程、指导流程、监督流程等。

(二) 数据安全管理层

管理层主要基于治理层的战略决策和体系设计负责数据安全治理体系的具体建设，包括管理体系、技术体系、流程体系建设，及指导体系的落地执行。在**管理体系建设**过程中，包括了根据治理层设计，对职能架构和组织结构的组建，定岗定责等活动。**技术体系建设**主要结合治理层制度体系架构的设计思路，从数据行为安全、数据内容安全、数据环境安全等方面开展的系列规范性约定的活动，**流程体系建设**定义和制定了各项活动具体执行需遵循的流程，如数据资产管理流程、安全需求定义流程、策略制定执行流程、监控与审计流程、治理能力评价流程等。是承上启下的一层，对上贯彻和落实决策层的意志和决策，对下指导和规

范执行层的行为。

(三) 数据安全执行层

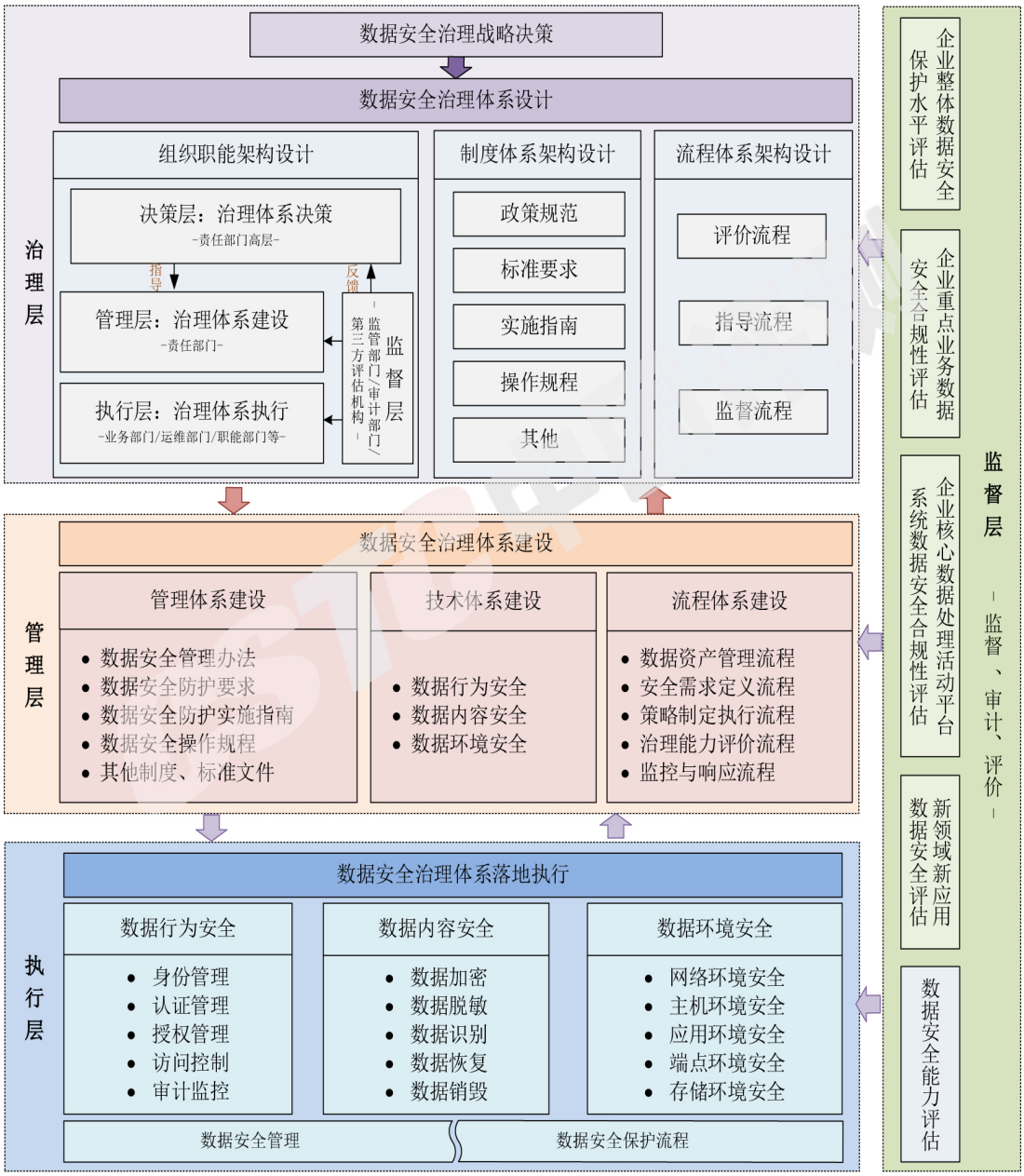
执行层将数据安全的技术手段分为从数据行为安全、数据内容安全和数据环境安全等方面，以全面支持管理层各体系的落地执行。其中数据行为安全主要包括身份、认证、授权的管理，访问控制及审计监控等技术管控手段；数据内容安全包括数据加密、脱敏，数据识别以及数据恢复和销毁等技术防护手段；数据环境安全包括网络、主机、应用、端点、存储等方面的环境安全。数据安全管理和数据安全保护流程支撑贯穿了整个执行层，指导、规范各项执行活动。该层是技术能力和人员意识的密集养成层和体现层，也是数据安全治理需求的主要提出层，第三方安全服务商提供的数据安全解决方案绝大部分集中在该层。目前行业内的防护执行主要采用以系统或网络为单元的“网元”模式。

(四) 数据安全监督层

监督层主要活动为对数据安全治理体系设计、建设和运行情况的监督、审计和评价，包括了监管部门的监督管理工作，安全审计部门的专项审计以及第三方机构的安全评估工作等，并向决策层、管理层按流程反馈体系运行情况及执行层的数据安全治理需求等，促进整个体系的持续优化。就目前行业的监管要求来看，监督层的活动应至少包括数据安全专项监督治理、企业整体数据安全防护水平评估、企业重点业务数据安全合规性评估、企业核心数据处理活动平台系统数据安全合规性评估、新领域新应用数据安全评估以及《GB/T 37988-2019 信息安全技术 数据安全能

力成熟度模型》要求的数据安全能力评估等工作。

图 3：数据安全治理体系框架



图片来源：中国评测网安中心，2020 年 7 月

七、电信和互联网行业数据安全治理建议

(一) 政策协调为逻辑起点

建立系统、明确的数据安全治理体系框架，是指导行业更规

范有效进行数据安全治理的前提，也是行业目前迫切需要开展的工作。无论是立足国情放眼国际的差别性顶层设计，还是基于行业性质的利益平衡规则构建，都要将确保政策体系的整体协调，作为行业数据安全治理及其体系框架构建的逻辑起点。

首先，要立足国情，遵循国家现行相关法律法规、政策标准，跟进并接轨正在立法阶段的《电信法》、《数据安全法》、《个人信息保护法》等法律法规；

其次，要基于行业，与现行行业政策、法律法规、行业标准互补、兼容，并推陈出新，同时注重与国内政策的体系化综合运用；

再者，不容忽视的是对动态复杂的全球数据治理态势和规则的研判、分析，尤其涉及数据跨境，须明确治理立场，政策法律宣示兼以程序设定、公共监管兼以行业自律，提高政策确定性和可操作性，提升国际市场信任水平。

(二) 权责分明为框架主线

数据安全治理较数据安全管理，意味着更顶层的战略决策、更合理的权责安排及更严密的问责机制。行业应将参与数据要素市场的各方主体，包括但不限于主管部门、行业相关企业或组织、行业数据拥有者等，在治理体系中明晰的权利和责任作为行业数据安全治理体系框架的主线。

尤其是针对数据拥有者权益的合理衡量和务实便利的权益变现，可作为行业数据安全治理的理念特色，因为从国家或行业监管层面，不管是《民法典人格权编》，还是《个人信息保护法》、

《数据安全法》等相关法律法规，用户隐私权及其他数据权益的依法正当化维护已是趋势。

在企业层面，应区别于前期由单个或个别部门驱动治理的模式，须有高层参与从对治理体系战略目标、范围、策略的决策，到对治理体系的建设，再到对治理体系运行的监督、反馈等不同层级的组织建设及定岗定责。其中建设层面应包括管理制度的建设和技术手段的建设，数据安全的需求也多源于该层面的反复实践。纵向的定岗定责和各层级横向的定岗定人，结合合理分明的权责安排和问责机制，形成企业数据安全治理的主轴线。

(三) 分级分类为实践基础

数据分类分级是差异化安全策略制定和精细化安全管控的基础，是数据安全治理实践的基础。“网元”模式有分类分级的加持，可统筹考虑“网元”与其承载数据的安全级别，尽量避免安全需求与安全等级措施的不匹配问题。

监管部门制定行业数据分类分级制度规范，指导协调各参与主体开展数据分类分级工作。企业层面，综合考虑数据主体、业务属性、用途、安全需求等因素，对数据资产的使用情况、权限状态、使用分布等进行系统全面的梳理，并按照一定的原则和方法进行分类和标识，在企业层面形成行业数据分类清单，明确数据安全主体责任及防护边界；在分类标识的基础上，综合分析数据的保密性、完整性、可用性和可控性等属性遭到破坏后可能对国家安全、经济运行、社会秩序、公众利益的危害程度，进行数据逐类安全定级和标识，明确各级别的安全需求配套相应保障措

施，实现分级管理。数据拥有者根据其数据分类分级情况，维护相应权益。

低级别、权属相对清晰的数据可以优先进入市场，促进数据更大空间的流动、共享、交易和使用，而对高级别的数据可以重点防护，在配备相应安全保护措施保障数据安全的前提下最大限度地释放数据价值。

(四) 治理评估为落地支撑

政策、体系、制度终需落地，并在监管过程中发现企业或组织在组织建设、制度流程、技术工具和人员能力等方面的数据安全能力差距并持续优化。数据安全治理能力直接反映数据安全治理主体当前实践、流程、方法的能力水平，并影响相关主体对治理主体的治理信心。而数据安全治理能力的评估是发现能力差距、评价数据安全治理程度和效果的关键方法。

根据工信部印发《关于 2020 年电信和互联网行业网络数据安全管理管理工作的通知》，行业数据安全治理的评估工作至少应包括企业整体数据安全防护水平评估、企业重点业务数据安全合规性评估、企业核心数据处理活动平台系统数据安全合规性评估、新领域新应用数据安全评估等工作。

此外，《GB／T 37988-2019 信息安全技术 数据安全能力成熟度模型》分别从安全能力、能力成熟度等级、数据安全过程三个维度定义了数据安全能力成熟度模型（DSMM）,行业可结合自身特点，在上述行业数据安全评估的基础上，参考 DSMM，规范和指引行业通过自评估或有相应服务能力的第三方机构开

展数据安全治理能力评估工作。

通过调研与访谈、查阅与演示、测试与验证等方式，对企业或组织开展数据安全组织建设、制度流程、技术工具和人员能力等方面的综合评估，分析其资产梳理差异、合规性差距、安全能力差距等，并提出相关建议，最后以数据安全治理能力综合评估报告反馈，为数据安全治理工作机制持续优化提供参考。

网络空间安全测评工程技术中心

地　址：北京市海淀区紫竹院路 66 号赛迪大厦 4 层

传　真：86-10-88559332

手　机：86-17310065881（白利芳）

86-18600832592（朱信铭）

邮　箱：bailifang@cstc.org.cn（白利芳）

zhuxm@cstc.org.cn（朱信铭）