中移智库

企业跨境数据流动安全合规白皮书

（2023）

中国移动通信有限公司研究院

2023年2月

前 言

数据作为新型国家战略性资产，其经济价值与战略价值在全球数字经济发展过程中日益凸显。作为维系全球经济活动的重要纽带和经济新秩序博弈焦点，跨境数据流动在大力推动经济全球化发展的同时，也面临数据安全保护、数据监管合规等方面的问题与挑战。随着世界各主要经济体对跨境数据流动提出越来越多的监管要求，如何合规开展跨境数据流动已不是企业面临的“选答题”，而是“必答题”。当前我国企业跨境数据流动合规保障体系还处于起步阶段，企业日益频繁的跨境数据流动需求、日趋严格的跨境数据流动监管要求与跨境数据流动合规保障能力尚不匹配。

本白皮书基于当前全球跨境数据流动主流模式及安全合规方法论，面向企业提出一套以“管理体系、技术体系与运营体系协同发展”为核心的企业跨境数据流动安全合规指导方案。白皮书力图满足市场需求，为企业提供组织、制度、流程构建等方面的指引，优化跨境数据全流程管理，促进跨境数据安全合规流动。

本白皮书由中国移动通信有限公司研究院主笔，中国移动国际有限公司、启明星辰信息技术集团股份有限公司联合编写。

目录

1 企业跨境数据流动风险态势

1.1 企业跨境数据流动需求与意义

全球正加速迈入数字经济时代，数据成为驱动经济发展的关键生产要素。跨境数据流动已成为推动经济全球化与国际贸易发展的重要力量。自2008年以来，跨境数据流动对全球经济增长的贡献已经超过传统的跨国贸易和投资，支撑了包括商品、服务、资本、人才等其他几乎所有类型资源的全球化活动，而且开始发挥越来越独立的作用[1]。党的二十大报告专门提出“推动货物贸易优化升级，创新服务贸易发展机制，发展数字贸易，加快建设贸易强国”的重要任务。作为驱动数字经济发展的重要力量[2]，数据跨境流动将重塑各国劳动力市场竞争关系及价值链，在促进我国贸易增长、加速技术创新等方面发挥重要作用。

企业作为市场主体，其业务模式和经营模式引发高频化、规模化且常态化的跨境数据流动。在全球产业分工日趋细化的背景下，企业的海外业务布局通常涉及多个国家，数据的集中协同处理是企业经营的客观需求。依托数字技术和信息网络，企业跨境数据流动可促进各类资源要素畅通流动以及各行业市场主体加速融合，帮助企业持续推动自身运营方式改善、供应链优化与商业模式创新，助力企业实现资源的高效配置。

本白皮书重点关注我国境内企业开展跨境数据流动所面临的形势、困难与问题，提出促进跨境数据流动安全、有序、合规开展的指导方案。

1.2 企业跨境数据流动现存问题

随着企业数据跨境传输、访问、使用的频次和容量大幅度上升，数据跨境流动所带来的风险越来越复杂。当前企业跨境数据流动面临“规则异”、“识别难”与“风险高”三大挑战，难以实现安全与效益的平衡。

1.2.1 跨境数据流动“规则异”

跨境数据流动面临数据流出国与流入国之间在数据保护、数据监管等方面的法律法规冲突。各国均以维护本国利益为出发点，构建跨境数据流动法

律条款和监管制度。美国跨境数据流动以维护其在全球贸易中的主导地位为核心，以“自我赋权”延展自身在全球范围内的数据主权辖域[3]。欧盟以大数据单一市场战略打造欧盟数字经济整体实力，采用单边立法赋权方式扩张其长臂管辖权[4]。我国遵循“数据境内存储，出境安全审查”模式[5]，通过三部上位法明确数据出境安全管理基本原则。在各个国家与地区跨境数据流动法律法规的多重管辖下，企业在实践层面面临规则不统一、差异大的难题。

1.2.2 跨境数据流动“识别难”

随着数字贸易的蓬勃发展，跨境数据的种类和数量呈现指数级递增。对海量数据进行全面梳理分类和有效识别是实现跨境数据流动合规保障的前提。依据我国《网络安全法》、《数据出境安全评估办法》等法律法规要求，企业需要识别跨境数据在境内、境外的分布状态，并对数据进行分类分级标识，对核心数据、重要数据、个人信息等进行重点安全防护，建立境内、境外数据分类分级防护能力体系。数据跨境后企业为保护相关数据，需要全面了解敏感数据资产存储数量、位置及分布情况，制定切实可行的跨境数据安全防护策略。由于企业跨境数据规模大、种类多、速度快、频度高，如何准确高效进行数据识别成为企业在实践中面临的难点问题。

1.2.3 跨境数据流动“风险高”

随着企业数据价值的不断攀升，跨境数据攻击愈加频繁，且攻击者组织形式趋于集中化、专业化，攻击对象呈现多样化、泛在化，攻击方式走向智能化、多样化。企业在数据使用中根据不同的业务场景采取相关的数据安全保护策略和保护措施，以满足国内相关法律法规要求和境外数据使用的要求，防止数据泄露带来国家安全隐患和企业经营损失。随着数据跨境攻击技术的不断升级，跨境数据攻击活动严重扰乱了企业跨境数据生态健康发展，大大提升了企业数据安全防护难度与风险。

1.3 研究框架

本白皮书秉承“以安全为中心、以价值为驱动、以数据创未来”的理念，提出跨境数据流动安全合规体系和应用体系。研究框架如图1-1所示。

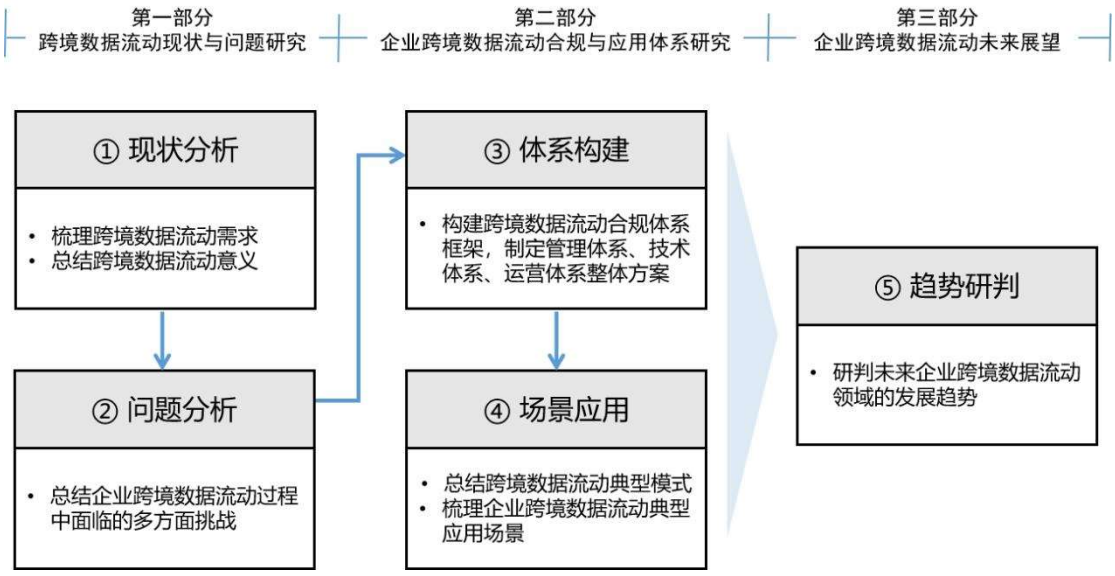

图1-1 研究框架

2 企业跨境数据流动合规体系

2.1 企业跨境数据流动合规总体框架

本白皮书以《信息安全技术-数据安全能力成熟度模型》(GB/T 37988-2019）[6]为基础，参考Gartner DSG（Data Security Governance）数据安全治理框架等多个业界主流模型[7]，面向《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》和《数据出境安全评估办法》中涉及到的企业跨境数据流动要求，从管理、技术与运营三个维度提出跨境数据流动合规体系，如图2-1所示。

2.1.1 跨境数据流动管理体系

跨境数据流动管理体系主要包括组织建设和制度规范建设。

跨境数据流动组织建设：首先要成立专门的跨境数据流动安全合规部门，以确保跨境数据流动安全合规工作的有效落实。

跨境数据流动制度规范建设：在整个跨境数据流动过程中，需要制定相应的安全策略和制度规范，所有的工作流程和技术支撑都需要围绕此规范制定和落实。

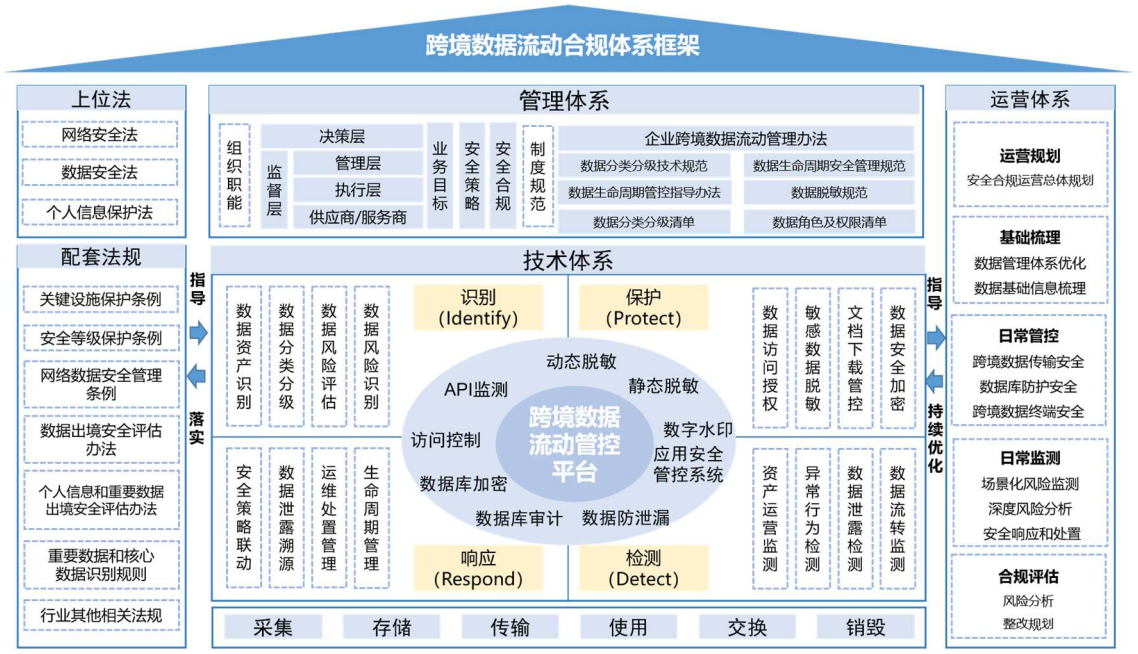

图2-1 跨境数据流动合规体系框架

2.1.2 跨境数据流动技术体系

跨境数据流动技术体系主要由管控平台和支撑能力组件共同构成。

跨境数据流动管控平台：该平台用于分析展现跨境数据资产分类、分级及分布情况，有效监控跨境数据流转路径和动态流向，实现集中化数据管控策略管理，加强数据的全生命周期管理能力，对数据风险进行识别和态势分析，为数据安全运营管理工作提供支撑。

跨境数据流动支撑能力组件：支撑能力组件包括动态脱敏、静态脱敏、API 接口监测管理等，为数据安全日常管理提供支撑，为数据全生命周期场景提供保护。

2.1.3 跨境数据流动运营体系

跨境数据流动运营体系由专业的运营团队提供服务，支撑管理体系与技术体系建设，开展日常管控与监测、合规评估等工作。

2.2 企业跨境数据流动管理体系

2.2.1 跨境数据流动组织建设

跨境数据流动组织职能需按照决策层、管理层、执行层、供应商/服务商、监督层的设计思路，在具体执行过程中，组织也可赋予已有团队与其它相关部门跨境数据流动的工作职能，或通过第三方专业团队开展工作。

（一）决策层

决策层是跨境数据流动管理工作的决策机构，建议由高层领导担任，参与组织的业务发展决策。其主要工作职责包括：

（1）制定组织的跨境数据流动目标和愿景；

（2）跨境数据流动策略、规划及发布；

（3）为组织的跨境数据流动体系建设提供必要的资源；

（4）对本单位跨境数据流动的重大事项进行协调和决策。

（二）管理层

管理层是跨境数据流动组织机构的第二层，基于决策层给出的策略，对跨境数据流动实际工作制定详细方案，做好业务发展与跨境数据流动之间的平衡。管理层在组织中发挥承上启下的重要作用，负责做好跨境数据流动全面落地工作，是组织内开展跨境数据流动工作最核心的部门或岗位。部分工作可能需要组织外部的专业资源来共同完成。

（三）监督层

监督层负责定期监督审核管理层、执行层和合作伙伴对跨境数据流动制度与管理要求的执行情况，并且向决策层进行汇报。监督层人员需具备独立性，不能由管理层、执行层等人员兼任，建议由组织内部的审计部门人员担任。

（四）执行层

执行层与管理层是紧密配合的关系，其职责主要是聚焦每一个跨境数据流动场景，对设定的流程逐个实现。执行层主要包括跨境数据流动专职人员和各业务部门的数据安全接口人员、风险管理人员、数据所有者等，其主要工作职责包括：

（1）负责跨境数据流动风险的评估和改进；

（2）负责管理跨境数据流动运营工作，例如，跨境数据风险自评估等事项审批；

（3）负责跨境数据流动重大事项的跟进和处理；

（4）协助跨境数据流动管理团队开展数据分类分级、重要数据识别等工作；

（5）负责跨境数据流动项目管理和实施。

（五）跨境数据流动部门协同

跨境数据流动组织机构和企业内多个部门之间有非常紧密的关系。在组织职能的顶层设计层面，业务部门、安全管理部门、运维部门等需要参与到策略方向及重大事件的决策中。在实际跨境数据流动工作开展层面，从平台底层设计到流程制定实施、人员安全管控、数据安全合规、对外披露等方面均需要相关部门深度介入和协作。

跨境数据流动管理层需要制定其与各部门之间的工作机制，目的是为了保障跨境数据流动工作顺利开展，例如跨境数据流动团队与业务方、法务以及合作伙伴之间的日常工作交流、争议与问题解决等事项。

2.2.2 跨境数据流动制度建设

在进行跨境数据流动管理制度和规范设计时，范围应覆盖跨境数据的全生命周期。企业可以参考跨境数据流动的相关要求、行业法规、顶层设计以及标准规范等，建立企业内部制度规范，约束和规范相关人员开展日常工作，并赋予管理人员监督管理职责，如图2-2所示。

制度流程需要整体考虑并形成体系框架，制度体系需要分层，层与层之间，同一层不同模块之间需要有关联逻辑，在内容上不能重复或矛盾。一般可分为四级。

（一）一级文件

一级文件包含方针、策略、基本原则和总的管理要求，主要内容包括但不限于：

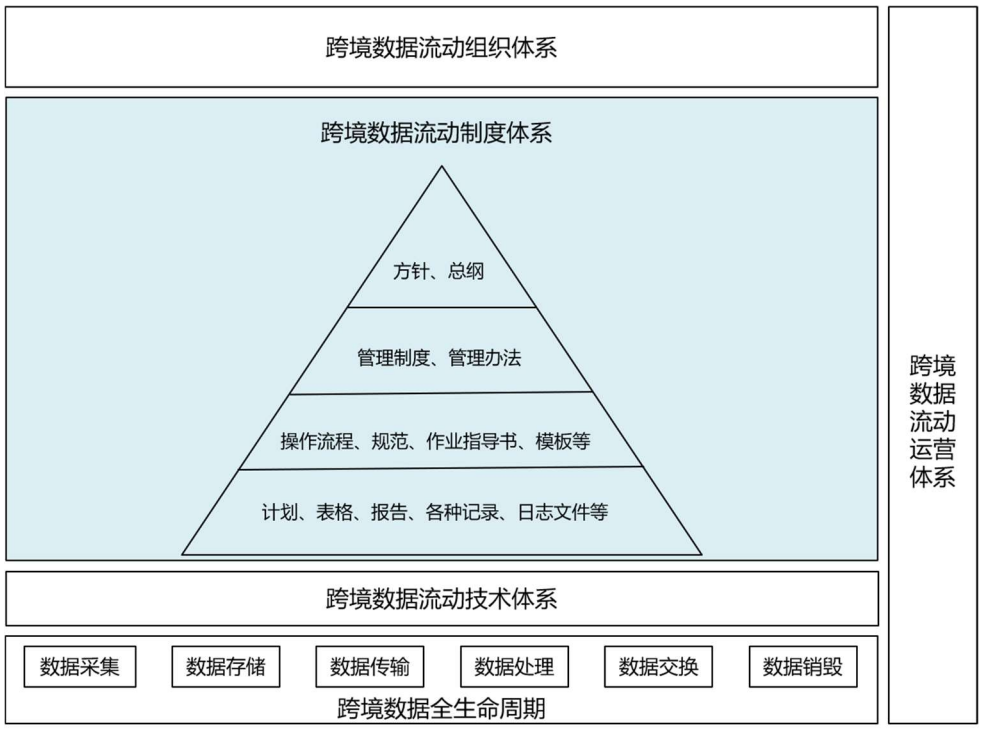

图2-2 跨境数据流动制度流程

（1）跨境数据流动管理的目标、愿景等；

（2）数据及数据资产定义：例如定义数据类别、个人信息、重要数据、信息系统载体等；

（3）跨境数据流动管理基本原则：例如跨境数据分类分级原则、跨境数据流动和业务发展匹配原则、跨境数据流动管理方针和政策等；

（4）跨境数据生命周期阶段划分和整体策略：例如数据产生、数据存储、数据传输、数据交换、数据使用、数据销毁等；

（5）跨境数据流动违规处理：例如违规事件及其等级定义、相应处罚规定等。

（二）二级文件

二级文件包含跨境数据流动管理制度和办法。跨境数据流动制度和办法是指跨境数据流动通用性要求、各生命周期阶段中某个或多个方面的规章制度要求，例如：

（1）通用性要求：数据资产管理、数据质量管理、数据安全合规管理、

系统资产管理等；

（2）跨境数据生命周期各阶段：数据采集管理、数据存储管理、数据传输管理、数据交换管理、数据使用管理、数据销毁管理，以及某个特定方面的管理要求等。

（三）三级文件

三级文件包含跨境数据各生命周期及某个特定方面的操作流程、规范、相应的作业指导书、指南及配套模板文件等。

在保证生命周期覆盖完整的前提下，不需要每个方面或者每个生命周期阶段都单独建立流程和规范，可以根据实际情况整合流程和规范文档。跨境数据流动操作指导书或指南是对跨境数据流动管理流程、规范的解释和补充，以方便执行者深入理解和执行，并非要求强制执行的制度规范。

跨境数据流动模板文件是与管理流程、规范和指南相配套的固定格式文档，确保执行一致性。

（四）四级文件

四级文件指执行跨境数据流动管理制度产生的相应计划、表格、报告、各种运行或检查记录、日志文件等。

2.3 企业跨境数据流动技术体系

依据多级管理思路对跨境数据流动技术体系进行建设。企业境内总平台以建设跨境数据供给区为主要内容，企业境外子平台以建设跨境数据管控子平台、跨境数据能力组件为主要内容。

2.3.1 境内总平台建设框架

跨境数据供给区主要进行跨境数据供给，统一为境外子平台提供数据采集服务，该区提供数据脱敏、数据接口管控、数据获取权限控制等能力，如图2-3所示。

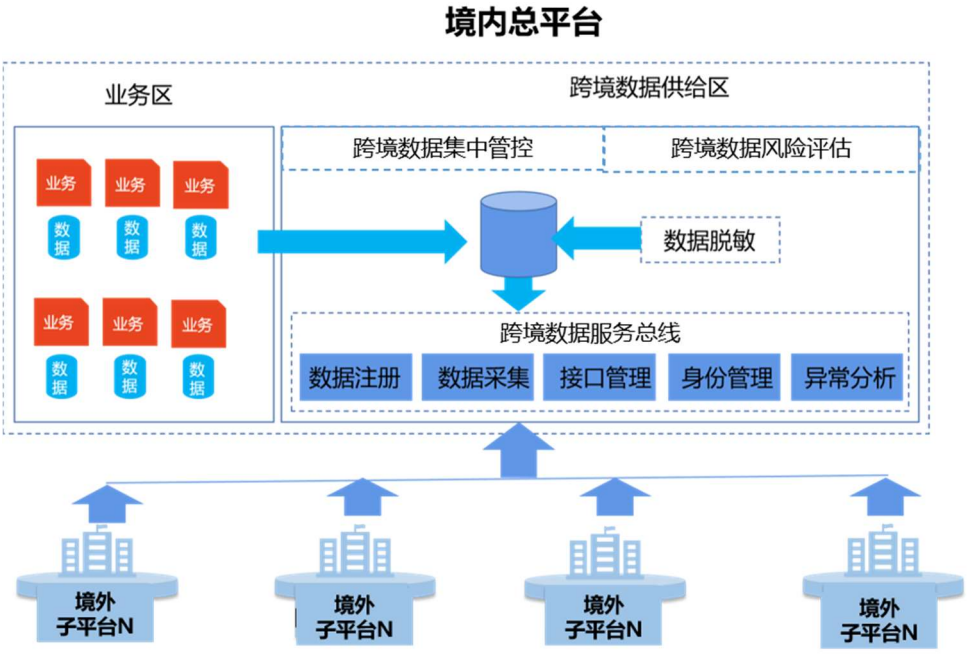

图2-3 境内总平台建设方案示意图

（一）跨境数据服务总线

跨境数据服务总线用于满足跨境数据资源共享与服务交换需求，系统整合数据供给渠道，实现统一、开放、安全、规范的信息交换体系，主要内容包括：跨境数据资源统一注册、接入适配、协议转换、服务调度、访问控制、安全认证、红名单配置、日志审计、系统资源监控等。

（二）脱敏系统

跨境数据库脱敏系统针对用户数据进行高仿真处理，对敏感数据进行脱敏。功能包括：数据抽取、敏感信息自动发现、脱敏、装载。主要适用场景为：数据导出外发、数据测试、数据挖掘分析等。

自动化脱敏流程主要包括：生产数据库数据提取、敏感信息自动捕获、敏感信息转换变形、脱敏后数据回写。脱敏流程需包含分级审批、审核的机制，以适应多种应用场景和管理需求。

（三）境内总平台集中管控

企业境内总部管控平台承担企业跨境数据集中管控职能，支撑跨境数据业务的数据安全合规工作，包括：数据供给管控、子平台数据使用管控、数据安全策略、数据保护能力、数据风险管理、跨境数据风险评估安全上报等。

2.3.2 境外子平台建设框架

境外子平台包括跨境数据管控子平台、跨境数据能力支撑组件建设两部分。跨境数据流动管控子平台对企业境外子公司数据安全资产、数据安全策略、数据安全能力进行统一管理，对跨境数据使用情况和风险进行上报。跨境数据能力组件围绕具体业务场景对境外子公司的数据安全行为进行保护。

（一）境外子平台集中管控

跨境数据流动境外子平台向上承接国内总部安全策略，上报资产数据、策略数据、数据流转信息、风险日志等。向下为子公司数据安全管控提供支撑，包括数据安全视图管理、数据资产管理、数据安全策略管理、数据流转监控、数据风险监测管理、数据全生命周期管理和数据安全合规管理等功能。

（二）境外子平台能力支撑组件

（1）接口API监测系统。主要功能包括：接口信息采集、异常访问行为监测、页面访问频次监测与敏感信息访问监测等。

（2）静态脱敏系统。针对用户数据进行高仿真处理，对敏感数据进行脱敏。主要功能包括：数据抽取、敏感信息自动发现、脱敏、装载。主要适用的场景为：数据导出外发、数据测试、数据挖掘分析等。

（3）核心信息管控系统。该系统提供统一、集中的授权、访问控制和运维审计平台，通过云端管理的方式对企业存在的跨境数据风险实现控制。

（4）跨境数据安全审计。主要功能包括：针对不同的数据库协议，提供基于应用操作的审计；提供数据库操作语义解析审计，实现对违规行为的及时监视和告警；提供缺省的多种合规操作规则，支持自定义规则（包括正则

表达式等），实现灵活多样的策略和响应；提供基于硬件令牌、静态口令、Radius支持的强身份认证；根据设定输出不同的安全审计报告等。

（5）动态脱敏系统。支持敏感数据的自动发现，内置脱敏算法和敏感数据类型。

（6）终端管理系统：包含终端防护和数据外发管控两部分。终端防护主要功能包括：对所有要离开终端电脑的数据进行扫描；支持客户端提交文件外发审核申请；针对敏感外发事件通过邮件自动发送到指定邮件地址；详细记录敏感事件产生的原因及终端信息；把外发敏感的文件上传到服务器备份。数据外发管控主要功能包括：基于终端进行多种泄密途径的监控，对系统中的应用程序进行敏感数据外发管控。

2.4 企业跨境数据流动运营体系

2.4.1 跨境数据流动运营体系规划

对跨境数据业务系统及运行现状进行调研，梳理企业跨境数据管理制度，立足企业跨境数据规则与国家跨境数据管理条例差异，制定与企业相契合的跨境数据流动运营总体建设方案。

2.4.2 跨境数据流动基础信息梳理

（一）跨境数据流动管理体系优化

明确企业待保护内容、识别敏感数据，进行针对性防护，持续优化企业制定的跨境数据管理制度规范。

（二）跨境数据基础信息梳理

对企业跨境数据流动的系统、业务及跨境数据等关键资产进行发现、梳理、识别、分级分类等工作。分级分类维度包括：数据对业务系统的影响程度、数据丢失后对企业的影响程度、数据的业务属性、数据敏感级别、数据类型、使用权限等。

进行跨境数据基础信息梳理时，需基于调研形成数据资产清单及跨境数据流动规范。调研内容包括：相关跨境数据流动规范、现存业务内容及业务流程、跨境数据存储和使用情况等，如图2-4所示。

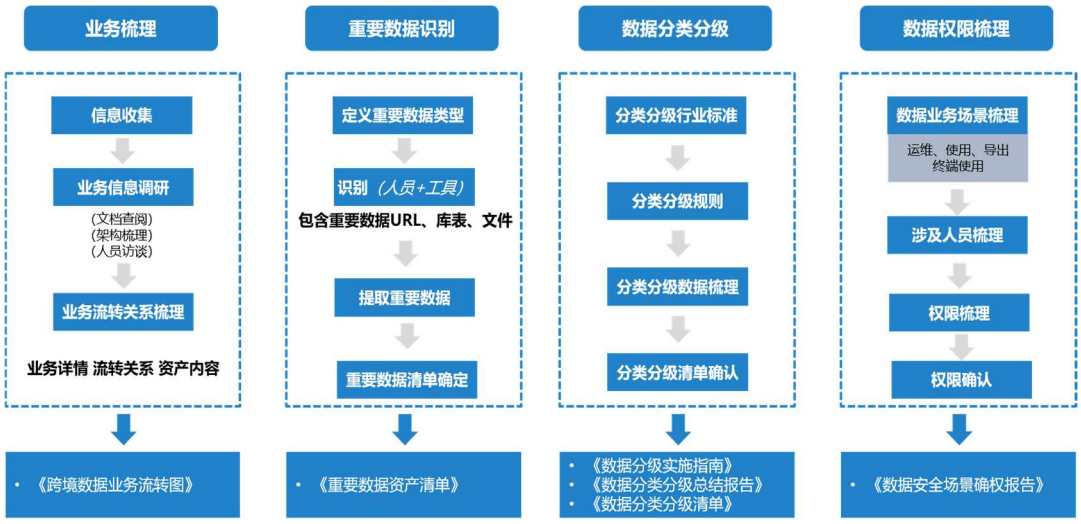

图2-4 跨境数据流动基础信息梳理示意图

2.4.3 跨境数据流动日常管控

企业需将跨境数据流动管理和技术实现交叉互融，确保跨境数据流动措施落地实施。集中化管控需对跨境数据传输安全、跨境数据库防护安全、跨境数据终端安全进行重点保护，通过审查机制提升运营能力，实现资源的统一调度及管控。

2.4.4 跨境数据流动日常监测

（一）场景化风险监测

企业需对敏感数据流动场景进行监测和审计，主要场景包括：敏感信息未脱敏化、无认证访问行为、参数篡改访问、低权访问高权业务、跨区域非法办理业务、账号复用、批量高频访问敏感信息等。

（二）深度风险分析

企业需基于异常行为规则和敏感信息访问规则，实现用户异常行为及敏感信息访问分析，协助定位安全事件、发现安全事件责任人、发现跨境数据泄露源，协助进行业务止损。

（三）跨境数据安全响应和处置

当企业业务系统遭受黑客入侵攻击、面临敏感数据资产泄露风险时，需第一时间对入侵事件进行分析、抑制、还原、处理、查找入侵来源并恢复系统正

常运行，输出应急响应报告。

2.4.5 跨境数据流动合规闭环评估

跨境数据流动合规闭环评估涵盖八个部分：

（一）调研访谈：调研问卷填写、高级管理层访谈、业务部门访谈、数据安全部门访谈、支撑保障部门访谈等。

（二）文档核验：组织职能、管理制度、业务流程、合同协议、IT 流程、应急响应等。

（三）资产梳理：出境业务调研、相关系统梳理、数据资产盘点、数据传输方式调查、企业跨境数据通道梳理。

（四）现场勘查：业务流程穿越测试、分类分级策略核查、脱敏策略核查、访问控制策略核查、数据库安全核查、服务器配置核查、安全设备核查。

（五）风险分析：部分结果判定、关联结果判定、风险分析模型。

（六）专家评审：业内专家评估、专家评审报告。

（七）整改规划：风险点整改建议、业务整改支持、中长期安全规划。

（八）自评估报告：自评估报告编制、申报书编制、其他材料整合。

3 企业跨境数据流动应用体系

在信息化、数字化、智能化的时代背景下，数据跨境流动活动普遍存在于企业各类商业需求和实务场景中。

3.1 企业跨境数据流动模式与应用场景

在跨境数据流动的实际应用中，不同企业的注册地、业务开展区域以及具体业务场景各有不同。数据跨境流动是双向的，可能面临境内向境外、境外向境内、境外向境外但途径境内等多种情况。根据数据的第一落点不同，可以将数据跨境流动划分为两种模式。第一种模式是数据第一落点在境内，再向境外提供数据，即数据主动出境。该模式下境内企业收集数据后向境外其他数据处理者传输，较为典型的场景如跨国公司或关联公司之间的业务数据共享、境内企业与境外服务提供商在业务合作中的数据传输、跨境电商向境外提供境内用户与订单数据等。第二种模式是数据第一落点在境外，即数据被动出境。该模

式下境外企业直接收集并处理境内数据，较为典型的场景如境外主体直接采集并处理境内个人信息以便提供服务或产品、开展用户行为数据分析等[8]。

3.1.1 模式一：境内企业收集境内数据后向境外传输

在第一种模式下，境内的数据处理者通过传输、存储、上载、递送等动作，将其在境内运营中收集和产生的数据提供至境外，这是数据出境中的常见方式。在此模式中，数据的第一落点为境内数据处理者，其在境内经营活动中收集的个人信息首先储存于境内服务器，再由境内主体转移至境外其他处理者，后续数据还可能在境外继续流转。

基于企业常见业务活动，企业在此模式下存在若干数据跨境流动典型场景，主要包括：

（一）跨国公司或关联公司间的业务数据共享。企业可能会根据管理及业务需要，从境内向境外提供其在境内处理的员工个人信息、客户个人信息、业务信息等。

（二）境内企业与境外服务提供商合作。境内企业可能出于业务合作需要，委托境外服务提供商进行数据处理或者与境外企业合作处理其在境内收集的数据，例如境内企业与境外保险机构、医疗机构开展合作，境内销售方委托境外出口管制筛查机构提供合规服务等。

（三）境内跨境电商向境外提供境内的用户和订单数据。跨境电商可能会向境外接收方提供完成订单所需的用户地址信息和身份信息等，也可能进一步提供用户的购物记录和浏览行为等额外数据。

3.1.2 模式二：境外企业直接收集并处理境内数据

在第二种模式下，境外数据处理者直接收集、存储产生于境内的数据。在此模式下，数据的第一落点为境外服务器，境外的主体直接收集境内数据，后续境外数据处理者也可能进一步向境内或境外的其他数据处理者提供其收集的数据。

在第二种模式下，企业常见的业务场景包括：

（一）以向境内提供产品或者服务为目的的境外公司收集数据。例如注册于境外的企业在境内并未设立分公司或者子公司，也无数据中心或服务器，但

是其营业范围包括向境内提供产品或者服务，并且在提供过程中收集个人信息向境外传输。

（二）境外主体直接收集境内数据进行评估分析。例如境外学校在招生场景下分析境内学生简历、境外企业招聘场景下分析境内简历，或者境外公司采集用户行为数据以编写行为习惯分析报告等。

3.2 企业跨境数据流动合规体系在典型场景中的应用

本白皮书重点研究我国境内企业开展跨境数据流动面临的问题与解决路径。以下以第一种模式为例，介绍企业跨境数据流动合规体系在典型场景中的应用。

3.2.1 实施全流程分级多节点集中管控

针对境内企业收集境内数据后向境外传输这种流动模式，可设定境内企业集中管理平台为总平台，以境外平台为子平台，实现统一集中的管理，对各子平台的数据使用情况进行策略管控，对数据进行监测，对数据风险进行分析。

3.2.2 建立集中的跨境数据供给区

建立统一安全的跨境数据供给区，通过接口访问、接口监测、接口权限管理、数据脱敏等技术对跨境数据进行统一归集管理。

3.2.3 开展场景化的跨境数据管控

企业需以数据为中心基于场景化的思路，根据具体场景开展跨境数据流动管控。企业一方面要遵循公司跨境数据流动管控和上级单位监管方面的场景要求，另一方面要围绕跨境数据出境后在境外子平台数据使用的相关场景开展数据安全保护，防止数据泄露。以身份为中心围绕跨境数据的采集、存储、使用等场景，对接口、人员进行基于身份的行为管控。

（一）跨境数据采集场景

业务场景：通过接口在境内采集数据，用于业务处理。

潜在风险：采集接口缺乏有效管控，存在异常连接、恶意连接风险。

管控措施：总平台建立跨境数据供给区，采用数据总线对接口进行身份和鉴权管理，对跨境数据进行基于场景的脱敏管理，对数据分类分级进行管理。子平台通过API接口监测、数据库审计监测相关行为，发现异常接口。

（二）跨境数据存储场景

业务场景：跨境数据在企业内部存储。

潜在风险：敏感数据未标识且分布位置不明。

管控措施：识别敏感数据，并对数据分级分类。

（三）跨境数据使用场景

业务场景：业务开发使用需要测试数据、业务人员访问业务系统、运维人员下载数据等。

潜在风险：业务人员恶意查询与导出数据，运维人员越权恶意访问、查询与导出数据，开发测试人员利用测试机会导出真实数据。

管控措施：针对业务访问、运维、开发测试等场景，分别采用静态脱敏、核心信息管控等措施。

3.2.4 建设跨境数据流动能力支撑组件

根据业务场景进行策略梳理和业务风险梳理，需明确跨境数据能力支撑组件策略。支撑组件策略也需要“以数据为中心，基于业务场景”进行制定，为跨境数据流动安全合规运营提供落地方案。场景化建设关键要素是“人”“业务”与“数据”。企业需要梳理实际业务相关场景，制定数据访问控制策略、脱敏策略、泄露策略等。

4 企业跨境数据流动未来展望

基于前述分析，清晰的规则指导与有力的技术支撑是迎接企业跨境数据流动所面临诸多挑战的关键路径。展望未来五年，在规则层面，跨境数据流动针对不同行业的实际需求与特征将不断完善细化，面向各行业、企业更具可操作性与指引性；在技术层面，以数据自动化分类分级、隐私计算与区块链等为代

表的相关技术将得到快速发展与广泛应用。在规则完善与技术发展的助力下，企业跨境数据流动安全合规管理效率将日趋提升。企业构建跨境数据流动合规体系的价值追求也将从“合规性驱动”转向“业务价值驱动”。

4.1 规则完善：跨境数据流动监管规则的行业化特征日趋凸显

进行科学清晰的数据分级分类是实现跨境数据安全有序流动的基础。由于数据分级分类与数据自身特征强相关，而数据资源本身及其应用场景在不同行业间存在较大差异。这就意味着未来随着企业跨境数据流动的持续开展，为了满足不同行业跨境数据流动的实际需求，无论是国家层面的法律、制度及规范，还是企业层面的技术方案，都将围绕不同行业典型数据类型及应用场景而不断细化与完善，不同行业的企业将获得契合自身行业特点与需求的规则遵循与技术支撑。预计金融、能源、制造、电商等全球化发展程度高、跨境数据流动量大的行业将率先建立并完善行业化的管理规则与技术方案。

4.2 技术发展：跨境数据流动相关技术日趋成熟并广泛应用

未来数据自动化分类分级、隐私计算及区块链等各类技术将快速发展，并在跨境数据流动的关键环节得到广泛而深入的应用。在数据资产梳理方面，数据分类分级技术将助力实现核心数据、重要数据、个人数据的高效识别以及与相应数据类别、数据安全等级的智能关联，从而大幅提升工作效率。在数据分析处理方面，隐私计算技术将在助力企业实现“数据可用不可见，原始数据不出域”等方面发挥日益重要的作用。预计越来越多的企业将通过跨境部署隐私计算节点来完成重要数据或个人数据的处理分析。在数据流动管理方面，区块链技术将有效助力实现跨境数据流动全生命周期的“防篡改、可追溯、可信任”，为国家及企业的监管审计工作提供有力的技术保障。

4.3 价值转变：合规体系建设将由“合规性驱动”转向“业务价值驱动”

未来企业关注点将从满足监管要求转向为企业发展产生实际效能。企业跨境数据流动合规体系建设将从合规性驱动转向业务价值驱动，从而让合规投入

从“成本投入”转变成“价值投资”。企业关注点的升级将驱动跨境数据流动合规体系围绕数据流通的全流程来开展安全防护和价值运营，在做好安全保障的基础上，还将在数据安全防护与业务价值赋能中寻求最佳平衡点，以充分激发应用潜能，进而充分实现企业跨境数据流动的最终目的 --“通过数据赋能提升企业效能”。

参考文献

[1] 麦肯锡全球研究院（MGI）.数据全球化：新时代的全球性流动[R].2016.

[2] 刘宏松，程海烨. 跨境数据流动的全球治理 ——进展,趋势与中国路径[J]. 光明网（国际展望），2020，12(6):26.

[3] 邓崧，黄岚，马步涛. 基于数据主权的数据跨境管理比较研究[J]. 情报杂志，2021，40(6):8.

[4] Theodore C ， Fabien T . EU－US negotiations on law enforcement access to data: divergences, challenges and EU law procedures and options[J]. International Data Privacy Law, 2021.

[5] 钟力，唐会芳，王雨薇. 从数据利用视角探讨数据出境安全问题[J]. 中国信息安全，2022(003):000.

[6] 国家市场监督管理总局,中国国家标准化管理委员会. GB/T 37988-2019 信息安全技术-数据安全能力成熟度模型[S]. 北京:中国标准出版社，2019.

[7] Marc-Antoine Meunier. Data Security Posture in 2017[C]. Gartner Security & Risk Management Summit 2017. Maryland:Gartner. 2017.

[8] 傅广锐，袁嘉琦. 数据跨境流动的合规之道—兼评数据跨境新规对数据跨境业务的影响. 2022.

中移智库公众号

中移智库网站